Mauro Santaniello

Sunburst. La grande eclissi della cybersecurity Usa

(doi: 10.53227/101179)

Rivista di Digital Politics (ISSN 2785-0072)
Fascicolo 1, gennaio-aprile 2021

Ente di afferenza:
()

Mauro Santaniello

Sunburst

La grande eclissi della cybersecurity Usa

SUNBURST. LA GRANDE ECLISSI DELLA CYBERSECURITY USA

In mid-December 2020, a private cybersecurity firm discovered an unprecedented cyber-hack that had compromised thousands of digital networks all over the world, including those in use by many US government agencies and departments. The article advances an analysis of this case in order to shed light on some crucial issues related to contemporary cybersecurity policies. More in detail, the case study focuses on two key political aspects that have proved to be controversial and fraught with consequences. The first one concerns political mechanisms such as blaming, attribution and retaliation, and their relevance for international norms regulating interstate conflicts. The second aspect relates to the recent emergence of a new cybersecurity paradigm, which is challenging both the economic logics upon which the global diffusion of digital networks was based in the 1990s and 2000s, and the technical logics that in the two previous decades (1970-80) had informed the design principles and the governance system of the early internet.

KEYWORDS *Cybersecurity, Cyber Warfare, Internet Governance, Sunburst, Solorigate.*

1. Introduzione

Nella primavera del 2020 tutte le agenzie governative statunitensi che si occupano di *cybersecurity* erano concentrate sulle imminenti elezioni presidenziali. In quei mesi, le truppe cibernetiche Usa erano schierate su due fronti. Da lì, sulla scorta delle esperienze del recente passato, si prevedevano le principali incursioni nemiche.

Sul primo fronte, quello delle piattaforme, si doveva proteggere l'opinione pubblica americana dalle manipolazioni di *fake news*, *filter bubbles*, *hate speech*, micro-profilazione, *dark-ads*, e tutto l'arsenale della comunicazione *user-targeted* dispiegato, nella tornata precedente, dall'internazionale sovranista per il tramite di Cambridge Analytica e non solo.

Mauro Santaniello, Dipartimento di Studi Politici e Sociali/DISPS - Università degli Studi di Salerno - Via Giovanni Paolo II, 132 - 84084 Fisciano, email: msantaniello@unisa.it, orcid: 0000-0001-5582-622X.

ISSN 2785-0072

Sul secondo fronte, c'era da mettere in sicurezza l'infrastruttura elettronica, online e non, da cui dipende l'ecosistema policentrico degli uffici elettorali dei cinquanta stati americani. La lunga storia di incidenti accumulata dai vari sistemi in uso (dalle *voting machine* agli scanner ottici per il conteggio delle preferenze, dal voto via email a quello espresso su siti web realizzati ad hoc per conto di questa o quella commissione), nonché la violenta delegittimazione che tali sistemi stavano subendo in quel periodo dal presidente uscente e candidato in corsa per il secondo mandato, rendevano lo scenario operativo particolarmente caldo ed esposto agli umori della campagna elettorale.

In quei mesi, però, il nemico bivaccava alle spalle delle linee difensive. Si era infiltrato, senza essere rilevato, nei centri di comando di quelle stesse agenzie di sicurezza schierate a protezione del processo elettorale, nelle reti dei ministeri-chiave, nei sistemi delle compagnie private di *cybersecurity* che hanno contratti con il governo statunitense per tenere al sicuro infrastrutture e dati. I nemici erano entrati persino nella rete dell'Ufficio di Presidenza, nei corridoi ottici in cui viaggiano le comunicazioni non classificate del comandante in capo. «È come se bombardieri russi avessero ripetutamente sorvolato l'intero paese senza essere avvistati», dichiarerà via Twitter il senatore Mitt Romney una volta che l'attacco sarà stato scoperto, nel dicembre del 2020[1].

In effetti, la complessità, l'ampiezza e la profondità del *cyber hack* segnalavano, sin dai primi dati disponibili, che l'attacco non aveva precedenti nella storia delle reti digitali, e che si era di fronte a uno dei più gravi colpi subiti dal governo statunitense nel «cyberspazio americano». In estrema sintesi, gli attaccanti si erano fatti largo nei server della società texana SolarWinds sfruttandone alcune sbalorditive falle di sicurezza[2]. Da lì avevano assunto il controllo dei sistemi che gestiscono gli aggiornamenti automatici di Orion, una piattaforma utilizzata da circa 300.000 organizzazioni in tutto il mondo per monitorare e gestire le proprie reti. Un software che, per poter svolgere le proprie funzioni, ha un accesso praticamente illimitato a tutte le risorse connesse a un network: server, dati, periferiche, dispositivi. Una volta assunto il controllo dei sistemi di aggiornamento, gli attaccanti hanno racchiuso un pezzo di codice sorgente ostile (*malware*) all'interno di due *updates* diretti alle piattaforme dei clienti, uno a marzo, l'altro a giugno. Le prime stime di Solarwinds parlano di 33.000 clienti che hanno effettuato il download degli aggiornamenti infetti, e di circa 18.000 server su cui il malware è stato effettivamente installato. Su

[1] Mitt Romney, Twitter, 17 dicembre 2020, https://twitter.com/SenatorRomney/status/1339679645533429761/photo/1.

[2] Una delle password utilizzate su un server di SolarWinds era 'solarwind123'.

gran parte di questi server, il malware, noto oggi come Sunburst o Solorigate[3], si è limitato a effettuare un'analisi dell'ambiente circostante per poi spegnersi definitivamente. Su altri server, invece, ossia su quelli che gestiscono le reti informatiche del triangolo di ferro della *cybersecurity* statunitense (governo, industria digitale e contractors), Sunburst ha riconosciuto il tipico scenario che stava cercando, e ha aperto un varco segreto, una *backdoor*, per consentire l'accesso a guastatori e spie. Fino a metà dicembre, quando l'attacco è stato finalmente scoperto dall'azienda di *cybersecurity* FireEye.

In questo breve contributo, gli eventi connessi al Solorigate verranno utilizzati come spunti per approfondire alcune tematiche chiave delle politiche di *cybersecurity* così come vanno costituendosi in tutti i Paesi avanzati del mondo. In particolare, due riflessioni verranno elaborate a partire dall'attacco in questione. La prima riguarda i meccanismi di *blaming*, *attribution* e *retaliation*; la loro rilevanza per le norme internazionali che regolano i conflitti armati; e le sfide che le peculiarità delle *cyber operations* pongono ai tradizionali sistemi di risoluzione dei conflitti tra stati.

Il secondo insight è relativo all'emergere di un nuovo paradigma di sicurezza cibernetica, che mette in crisi tanto la logica economica su cui si era fondata la diffusione globale delle reti negli anni 1990 e 2000, quanto la logica tecnica che nei due decenni precedenti (1970-80) aveva informato la progettazione dei primi network digitali, i loro principi di design, i loro sistemi di governance.

2. Russia, Russia, Russia...

L'operazione ostile, si è detto, viene scoperta a metà dicembre 2020 dalla società di *cybersecurity* FireEye. Quasi per caso. FireEye stava infatti indagando su un furto subito pochi giorni prima, quando qualcuno aveva sottratto dai suoi server un arsenale di vulnerabilità usate dall'azienda per testare le reti dei suoi clienti. Già in quella occasione, gli esperti della società californiana avevano puntato l'indice contro un gruppo di hacker russi legati ai servizi segreti di Mosca, catalogati tra le «minacce avanzate persistenti», *Advanced Persistent Threats* (Apt), al numero 29 (Sanger e Perlroth 2020).

L'Apt29, noto anche come Cozy Bear, è lo stesso gruppo che in estate era stato accusato dalle agenzie di sicurezza statunitensi, britanniche e canadesi di essere l'autore di numerosi attacchi ai laboratori farmaceutici occidentali che

[3] In questo approfondimento utilizzeremo il termine Sunburst con riferimento agli strumenti utilizzati nell'attacco informatico, e il termine Solorigate per riferirci allo scandalo pubblico provocato dalla scoperta dell'operazione ostile.

stavano lavorando al vaccino per il covid-19[4]. Il 13 dicembre 2020, FireEye comunica la scoperta della falla su Orion a SolarWind e al *Computer emergency readiness team* (Cert) della *Cybersecurity and infrastructure security agency* (Cisa), un'agenzia federale istituita da Trump nel 2018 sotto la supervisione del Dipartimento della sicurezza interna degli Stati Uniti d'America (Dhs). In questa occasione FireEye non nomina i russi, ma parla di un «attacco altamente sofisticato da parte di uno stato-nazione» (Mandia 2020). Lo stesso giorno la Cisa emette una direttiva d'emergenza che ordina a tutte le agenzie federali civili di disconnettere Orion dalle proprie reti a causa di un attacco da parte di non meglio specificati *malicious actors* (Cisa 2020).

Il 14 dicembre 2020 il presidente e Ceo di SolarWinds, Kevin B. Thompson, in ottemperanza al Securities Exchange Act del 1934, riporta l'incidente alla Securities and Exchange Commission. Nel report, Thompson afferma che SolarWinds non è stata in grado di verificare l'identità degli attaccanti, che «le è stato suggerito» che si tratti di «un attacco da parte di uno Stato nazione estero», e che sta collaborando con FBI, intelligence community e altre agenzie federali Usa (SolarWinds Corporation 2020). Nello stesso giorno, però, la stampa statunitense, con in testa il Washington Post, citando fonti governative anonime, attribuisce espressamente l'attacco all'Apt29 e al governo russo (Nakashima e Timberg 2020; Dianian *et al.* 2020). Il 18 dicembre 2020, nel corso di un'intervista al Mark Levin Show, il Segretario di Stato Mike Pompeo dichiara: «possiamo dire chiaramente che sono stati i russi». Il giorno dopo, però, Trump twitta:

> Il Cyber Hack è molto più grande nei Fake News Media che nella realtà. Sono stato pienamente aggiornato e tutto è sotto controllo. Russia, Russia, Russia è la cantilena prioritaria quando accade qualcosa, perché il Lamestream è, perlopiù per motivi finanziari, pietrificato dall'idea di considerare che possa essere stata la Cina. Potrebbe anche aver colpito le nostre ridicole voting machines durante le elezioni, che ormai è ovvio che io abbia vinto alla grande[5].

Una dichiarazione che spingerà di lì a poco il senatore repubblicano Mitt Romney a dichiarare:

[4] Si veda UK National cyber security centre (Ncsc) (2020).

[5] Donald J. Trump, Twitter, 19 dicembre 2020, https://twitter.com/briankrebs/status/1340376292856909824/photo/1. Il tweet originale non è più disponibile a causa del ban permanente inferto da Twitter all'ex presidente Usa per aver incitato l'assalto al Congresso del 6 gennaio 2021.

> Sono deluso dal commento del presidente. Ma credo che ormai dobbiamo riconoscere che il presidente non ci vede quando si tratta di Russia. La realtà qui è che gli esperti, la gente che comprende realmente come funzionano i nostri sistemi, e come funzionano i computer, il software, e così via, le migliaia e migliaia di esperti alla CIA, alla NSA, al Dipartimento della Difesa, hanno determinato che l'attacco viene dalla Russia (Caralle e Griffith 2020).

I russi dunque. Forse. Molto raramente, infatti, è possibile attribuire con assoluta certezza un attacco cibernetico sofisticato a uno specifico autore. Soprattutto nei casi in cui l'azione viene scoperta solo dopo molto tempo, e l'attaccante ha potuto coprire o manipolare le sue tracce. L'identificazione dei responsabili procede solitamente sulla base di indizi e congetture. Gli orari d'ufficio in cui avvengono gli attacchi, la lingua utilizzata per le annotazioni al codice sorgente dei malware, le tecniche di attacco o gli strumenti utilizzati dai diversi gruppi in passato, i modelli comportamentali elaborati per ciascun gruppo, le prove relative a casi precedenti. Questo aiuta senza dubbio i decisori politici a decifrare gli eventi e la loro portata, e fornisce coordinate di senso all'opinione pubblica. Ma un conto è il processo, tutto politico, di *blaming*, ossia di condanna pubblica del presunto colpevole, e un conto è il processo investigativo e giuridico di *attribution*, di attribuzione delle responsabilità legali di un attacco.

Su quest'ultimo piano, qualunque attaccante dotato di risorse sufficienti può facilmente riprodurre modelli attribuiti ad altri gruppi, disabilitando a priori il processo di formazione di prove inequivocabili o quanto meno attendibili. A inizio dicembre 2020, per fare un esempio a noi vicino, Piero Di Lorenzo, presidente della società Irbm di Pomezia che da luglio lavora al vaccino anti-Covid con Jenner Institute di Oxford e AstraZeneca, rivela a «la Repubblica» che da mesi i sistemi informatici della sua società sono bersagliati da attacchi *cyber* provenienti dall'estero (Tonacci 2020). I primi indizi (in particolare un indirizzo IP) portano ai russi, alla famigerata Apt29. Ma dopo due mesi di indagini, gli investigatori, raccogliendo ulteriori tracce, e triangolandole con gli esiti di precedenti inchieste internazionali, giungono a tutt'altra conclusione. Si tratta del'Apt10, alias Stone Panda. Sono i cinesi, che fingono di essere russi (Bulfon 2021).

L'indeterminazione relativa alle responsabilità di un attacco ha conseguenze importanti sui meccanismi di risoluzione e governo dei conflitti tra gli stati. Sia su quelli prodotti dal diritto internazionale (*ius ad bellum* e *ius in bello*), sia su quelli più propriamente politici (come la strategia della deterrenza e la dottrina della *Mutual Assured Destruction,* Mad). Per quanto riguarda i primi meccanismi, v'è ormai consenso sul fatto che, in tema di sicurezza, si ap-

plichino al cyberspazio i principi generali del diritto internazionale[6]. E che un attacco *cyber* che produca ingenti danni si configuri come «uso della forza» e «attacco armato», a prescindere dalla tecnologia utilizzata. Se l'attacco è condotto da uno Stato contro un altro Stato, lo Stato attaccato è dunque legittimato, a norma dell'articolo 51 della Carta delle Nazioni unite, a difendersi e reagire, da solo o assieme ai suoi alleati[7]. Le modalità della reazione, «retaliation» nel gergo internazionale della *cybersecurity*, sono diverse: *cyber-to-cyber*, se la rappresaglia colpisce i sistemi informatici dell'avversario attraverso operazioni che avvengono dentro la rete; *cyber-to-kinetic*, se le operazioni *cyber* colpiscono infrastrutture fisiche del nemico o comunque gli producono danni materiali; *kinetic-to-cyber*, se le risorse cibernetiche nemiche (data center, infrastrutture di telecomunicazione, centri di calcolo) vengono colpite con armi convenzionali. Ora, sebbene sia Obama che Trump abbiamo dichiarato, nel corso dei relativi mandati, di tenere disponibili sul tavolo tutte le opzioni possibili in caso di attacco *cyber* agli Stati uniti, nei fatti la difficoltà di attribuire un'operazione *cyber* a uno Stato nazione fa venir meno a monte l'applicabilità dello *ius ad bellum*, escludendo la possibilità che un'azione di risposta da parte dello Stato attaccato possa essere riconosciuta come legittima dalla comunità internazionale. Parimenti, le norme dello *ius in bello* stabilite dal diritto umanitario internazionale divengono di difficile applicazione. Non potendo determinare con precisione le strutture governative nemiche responsabili dell'attacco, lo Stato attaccato avrebbe difficoltà a motivare la selezione dei target delle operazioni di *retaliation*. Inoltre, se si considera che gli attacchi avvengono di norma attraverso reti e sistemi utilizzati anche e soprattutto a scopo civile (*dual-use*), la reazione dello Stato attaccato avrebbe alte probabilità di colpire la popolazione inerme, sfociando inevitabilmente in una violazione del diritto di guerra.

Le difficoltà di attribuzione univoca degli attacchi *cyber* rendono inefficaci anche i meccanismi politici che, in passato, hanno funzionato come stanza di compensazione di conflitti e tensioni internazionali. L'attuale corsa agli armamenti *cyber* è stata spesso paragonata alla corsa agli armamenti nucleari nel corso della guerra fredda. In quella occasione, però, la certezza dicotomica sull'identità di attaccante e attaccato in un eventuale *first strike* aveva condotto alla stabilizzazione di un equilibrio politico che si reggeva sulla dottrina della cosiddetta «distruzione mutua assicurata», e che rendeva la corsa agli armamenti essa stessa uno strumento di deterrenza. Nel caso delle operazioni *cyber*, invece, l'impossibilità di identificare con immediata certezza l'autore del primo attacco, combinata con una sfocatura strutturale dei confini tra agenti go-

[6] Su questo e sui seguenti passaggi, si veda il Manuale di Tallin (Schmitt 2013).

[7] *United Nations, Charter of the United Nations, Article 51*, https://www.un.org/en/sections/un-charter/chapter-vii/index.html.

vernativi e unità operative para-statali o addirittura private, rende impraticabili le strategie di deterrenza tradizionali. Detto in altri termini, la *cyber war* non sarà mai una guerra fredda. Anzi. Essa è e sarà sempre più una guerra caldissima, combattuta costantemente lungo frontiere mobili ed estemporanee, tra soggetti mal definiti – ibridi – che si affrontano da remoto alla velocità della luce.

Tornando al caso dell'operazione di infiltrazione condotta tramite Sunburst, nonostante l'accesa disputa politica interna connessa ai processi di *blaming*, e un trend generale di politicizzazione delle tematiche *cyber*, è improbabile che si giunga a un'attribuzione di responsabilità talmente chiara e provata da poter dar corso a legittime sanzioni o ripercussioni contro lo Stato responsabile degli attacchi. In questo caso, come in altri simili, è la politica, più che il diritto, a dover trovare nuovi meccanismi di composizione e governo dei conflitti che siano idonei ad affrontare le sfide del *cyberwarfare* e della corsa agli armamenti cibernetici.

3. Internet reset: l'alba (da est) di una nuova rete

Il fitto dibattito pubblico che si è sviluppato negli Usa a seguito della scoperta di Sunburst si è rapidamente sfilacciato sotto i clamori dell'assalto al Capitol Hill Building di Washington del 6 gennaio 2021. Divenendo al più un episodio, uno dei tanti, della saga trumpiana. Analisi e discussioni sono però continuate nel sempre più vasto network internazionale di esperti, studiosi e decisori di *cybersecurity*. La domanda-chiave in questo dibattito tutt'ora in corso è «come è potuto accadere negli Stati Uniti d'America?» La rassegna delle risposte evidenzia due nuclei critici.

Il primo, di tipo culturale, identifica la principale vulnerabilità del sistema in quella che viene definita «l'arroganza dell'eccezionalismo americano» (Perlroth 2021). Ritenendosi più furbi degli altri, è l'argomento, i vertici delle agenzie federali di *cybersecurity* si sarebbero concentrati eccessivamente sugli arsenali di attacco, disinteressandosi delle difese. Nel caso specifico, dalle interviste del «New York Times» a «personaggi-chiave dell'intelligence», si evince che l'attacco è stato lanciato da server situati dentro i confini statunitensi, e per questa ragione i «sensori di early warning collocati dal Cyber Command e dalla *National security agency* (Nsa) in profondità nei network stranieri per rilevare la preparazione di attacchi hanno chiaramente fallito» (Sanger *et al.* 2021). Il discorso sulla presunzione come origine delle vulnerabilità americane ricalca con impressionante precisione le narrazioni che dominarono il discorso pubblico statunitense subito dopo il lancio dello Sputnik da parte dei russi. Un

editoriale radio del gennaio del 1958, firmato da Gabriel Heatter e messo in onda dall'emittente Mutual Broadcasting System, recitava:

> Grazie, signor Sputnik! Non saprai mai che gran rumore hai fatto. Ci hai dato uno shock che ha colpito molte persone, forte come Pearl Harbor. Hai inferto al nostro orgoglio un colpo spaventoso. All'improvviso ci hai fatto capire che non siamo i migliori in tutto. Ci hai ricordato una parola americana vecchio stile, umiltà. Ci hai svegliati da un lungo sonno (De Groot 1993, 78)[8].

Un testo che sembra scritto da un commentatore di *cybersecurity* dei nostri giorni, in cui riecheggia lo shock dell'attacco a sorpresa che devastò la flotta del Pacifico statunitense ancorata nel porto di Honolulu il 7 dicembre del 1941. Un'analogia utilizzata, più di mezzo secolo dopo lo Sputnik, da Leon Panetta, Segretario alla Difesa nell'amministrazione Obama tra il 2011 e il 2013, quando coniò l'espressione «Cyber Pearl Harbor» per descrivere il rischio di un attacco digitale alle infrastrutture critiche nazionali (Stone 2019).

Il secondo nucleo tematico della discussione che si è sviluppata attorno al caso Solorigate evidenzia una sorta di conflitto, nelle politiche industriali digitali statunitensi, tra la logica economica della crescita (l'ossessione neo-liberale della Silicon Valley formulata di recente nel cosiddetto – ironia della sorte – *growth hacking*) e la logica geopolitica della sicurezza nazionale. La prima avrebbe soverchiato la seconda nelle scelte cruciali del management aziendale di SolarWinds. Come quando ha imposto un decennio di *spending review* sui sistemi e le pratiche di *cybersecurity*, triplicando d'altro canto i propri profitti annui dai 152 milioni del 2010 ai 453 milioni del 2019 (Gallagher 2020). O come quando ha delocalizzato lo sviluppo di parti importanti del proprio software nell'Europa dell'est (Lenthang 2021). La frizione tra gli obiettivi economici individuali e gli imperativi della *cybersecurity* è evidente anche in un fenomeno che ha assunto dimensioni allarmanti da tempo, e che è stato spesso chiamato in causa nella discussione su SolarWinds. Si tratta dell'emorragia di *cyberwarriors* dalle agenzie federali, la fuoriuscita massiva di personale addetto alla *cybersecurity* che va ad alimentare un mercato mercenario internazionale, spesso al servizio di regimi illiberali o connessi a frange del terrorismo internazionale (Perlroth 2021). Tale fenomeno spiegherebbe, a detta degli osservatori, perché ad accorgersi di Sunburst sia stata una compagnia privata come FireEye e non una delle tante agenzie federali di *cybersecurity* istituite negli ultimi venti anni dal governo Usa.

[8] Traduzione dall'inglese ad opera dell'autore, testo originale citato in De Groot (2006, 78).

Questi processi, però, rappresentano solo un lato della medaglia. Negli ultimi anni, sotto la pressione dell'ascesa tecnologica della Repubblica Popolare Cinese e delle misure di contrasto adottate dall'amministrazione Trump, il frame geopolitico delle «esigenze di sicurezza nazionale» ha sempre più spesso ridimensionato le pratiche e le aspettative del libero mercato globale. Si pensi ai ban presidenziali che hanno colpito prima Huawei e poi le App cinesi, e alle pressioni diplomatiche sugli alleati affinché facessero altrettanto nei propri piani di sviluppo del 5G. Si pensi, in Italia, alle leggi sul cosiddetto Golden Power, e in particolare all'articolo 1-bis del decreto-legge n. 21 del 2012, introdotto dal decreto-legge 25 marzo 2019, n. 22, che include espressamente le reti di telecomunicazione elettronica a banda larga con tecnologia 5G tra i settori in cui al governo è consentito l'esercizio dei poteri speciali[9]. O si pensi, ancora, al Decreto-Legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, che istituisce in Italia «un perimetro di sicurezza nazionale cibernetica»[10] comprendente organizzazioni pubbliche e private, e coordinato dal Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio dei ministri. Da questa prospettiva siamo a un punto di svolta nei processi di produzione di significati connessi al cyberspazio, che modifica visioni, strategie politiche e politiche pubbliche. L'immagine del perimetro è l'antitesi, la più stridente, di quel free flow of information che aveva guidato lo sviluppo e la diffusione di internet negli anni novanta. Ed è in linea con un processo di militarizzazione del cyberspazio che si concretizza in nuovo paradigma della sicurezza informatica. Il caso Solorigate offre più d'una testimonianza della radicalità di questo cambiamento. Innanzitutto, esso mostra come le agenzie governative e le compagnie di *cybersecurity* che si suppone lavorino per rendere il cyberspazio più sicuro, impieghino in realtà le proprie risorse nello sviluppo di hacking tools e nell'individuazione di vulnerabilità che, anziché essere segnalate e risolte, vengono tenute nascoste per essere utilizzate al momento opportuno. Spesso, poi, questi strumenti finiscono in mani sbagliate, a disposizione di criminali o persino di stati rivali. È quanto accaduto con il primo attacco a FireEye che, come si è detto, ha sottratto all'azienda un arsenale di strumenti di offesa *cyber* tale da dover richiedere circa 300 aggiustamenti (fixes). Ma è accaduto, più volte, anche alla famigerata Nsa, la stessa agenzia che, stando ai documenti resi pubblici da Edward Snowden nel 2013, avrebbe messo sotto sorveglianza elettronica praticamente l'intero pianeta. Alcune armi *cyber* dell'arsenale della Nsa, ad esempio, sono state «catturate»

[9] Tali poteri includono: l'opposizione all'acquisto di partecipazioni da parte di soggetti esteri, il veto all'adozione di delibere societarie, l'imposizione di specifiche prescrizioni e condizioni.

[10] Decreto-legge 21 settembre 2019, n. 105.

nel 2016 dai cinesi mentre si difendevano da un attacco americano ai loro sistemi, e successivamente impiegate in attacchi *cyber* ad alleati degli Stati Uniti in Europa e Asia (Sanger *et al.* 2019). Tra il marzo del 2016 e l'agosto del 2017, inoltre, un gruppo di hacker che si firma Shadow Brokers ha pubblicato una vasta collezione di exploits sviluppati dalla Nsa, esponendo le reti di tutto il mondo ad attacchi sofisticati provenienti da attori altrimenti inoffensivi. Nello stesso periodo, l'arsenale di hacking tools della Cia veniva rubato da ignoti e successivamente pubblicato da Wikileaks nell'archivio «Vault 7», assieme a una corposa documentazione, dalla quale si evince, ad esempio, che gli hacker dell'agenzia avevano sviluppato procedure operative per «apparire come russi» durante le loro incursioni *cyber* (Cohen e Marquardt 2020). L'istituzionalizzazione di un modello di *cybersecurity* votato alla compromissione della sicurezza delle reti emerge con candore quando gli uomini dell'intelligence Usa sentiti dal New York Times in merito al caso Solorigate ammettono di avere una rete di sensori installata «in profondità nei network stranieri». Sono, in altre parole, essi stessi autori di operazioni d'infiltrazione simili a Sunburst, e contribuiscono ad alimentare sfiducia e diffidenza tra i gestori e gli utenti delle reti. Il paradigma della *cybersecurity*, così come va configurandosi nel suo stretto intreccio con la sicurezza nazionale e le strategie di potenza degli stati, ribalta completamente il set di norme della comunità di ingegneri e informatici cui era stato affidato lo sviluppo dei protocolli di base di internet.

Alla fine degli anni Ottanta, poco prima che la rete venisse privatizzata e commercializzata dall'Amministrazione Clinton, quella comunità, operante attraverso una serie di nuove istituzioni come l'*Internet architecture board* (Iab) e l'*Internet engineering task force* (Ietf), aveva approvato un nucleo fondamentale di principi relativi alla sicurezza, che rendevano «non etico e inaccettabile qualsiasi attività che intenzionalmente: (a) cerchi di ottenere accesso non autorizzato alle risorse di internet; (b) danneggi l'uso della rete; (c) sprechi risorse (personale, capacità, computer) per condurre queste azioni; (d) distrugga l'integrità dell'informazione basata sui computer; (e) comprometta la privacy degli utenti»[11]. Nel 1991, l'Ietf aveva approvato il *Site security handbook*[12] che, rispetto all'alternativa tra, da un lato, interrompere un attacco per preservare la sicurezza della rete e, dall'altro, lasciar correre l'attacco per individuarne il responsabile, indicava una preferenza per la prima opzione. E nella versione aggiornata del manuale approvata nel 1997, si ravvisava un dovere morale, per tutti coloro che scoprissero vulnerabilità e malware, di informare i gestori delle altre reti che avrebbero potuto essere esposte agli stessi rischi[13]. Questa siste-

[11] Si veda Internet Activities Board (1989).
[12] Si veda Holbrook e Reynolds (1991).
[13] Si veda Fraser (1997).

matica propensione a privilegiare la sicurezza dei network rispetto alla conduzione di indagini per individuare gli autori degli attacchi caratterizza quella che Sandra Braman chiama «network political citizenship», che si distingue dalla «geopolitical citizenship» in quanto quest'ultima mette al centro del concetto di «buon cittadino» le necessità delle agenzie di law enforcement, dei governi, e del sistema delle relazioni tra stati (Braman 2013).

I cambiamenti cui stiamo assistendo, dunque, indicano che quella che fino a un decennio fa era una logica secondaria nello sviluppo del codice di internet, ossia la logica geopolitica, sta rapidamente diventando la logica dominante. Non solo a discapito della logica economica, che ha dominato il campo dell'internet governance per tutti gli anni novantae per buona parte del primo decennio del nuovo secolo, ma anche rispetto alla logica stessa dei network, a quei principi di governance e di design elaborati sin dagli anni settanta dalla comunità di ingegneri e informatici che progettano e realizzano le architetture fondamentali del cyberspazio.

Nel contesto di questa trasformazione, la questione politica prioritaria non è la corsa agli armamenti *cyber*, che pur dovrà trovare meccanismi di composizione delle tensioni. Ma, più in generale, l'emergere di un nuovo paradigma di sicurezza digitale, che si fonda sul primato dei governi nazionali, sull'opacità dell'azione statale, sulla segretezza, sul sabotaggio, sulla compromissione di sistemi, dispositivi e reti. A questo nuovo modo di pensare la sicurezza digitale, promosso, come si è detto, in primo luogo dalle principali potenze cibernetiche occidentali (i cosiddetti *Five Eyes*), si accompagna il tentativo, da oriente, di riscrivere i codici di internet. Tanto quelli informatici (standard e protocolli) quanto quelli giuridici (trattati e convenzioni). È su questi due piani intersecantisi che Russia e Cina, lontano dai clamori delle opinioni pubbliche nazionali, stanno combattendo la loro battaglia globale per il controllo della rete. Sul piano del design di standard e protocolli, la Cina, che ha sin dall'inizio sviluppato la sua rete più come una intranet che come parte di un network globale, ha di recente presentato all'*International telecommunications union* (Itu), l'agenzia delle Nazioni Unite che si occupa di standard per le reti telefoniche e satellitari, il progetto per un «Nuovo Ip». La proposta, ufficializzata nel settembre del 2019, prevede di sostituire i protocolli fondamentali di internet, il *Transmission control protocol* (Tcp) e l'*Internet protocol* (Ip), con «una nuova architettura di rete con sicurezza intrinseca». La proposta è stata bloccata nel dicembre del 2020 dalla forte opposizione di Unione Europea e Stati Uniti (Zorloni 2020), ma il carattere volontario dell'adozione dei protocolli lascia aperta la possibilità che Pechino introduca, nelle sue reti e in quelle che sta costruendo ovunque nel sud del mondo, un set di nuovi protocolli compatibili con il Tcp/Ip, ma con una filosofia di design completamente diver-

sa. Il fatto stesso di aver presentato la proposta a un'agenzia intergovernativa come l'Itu anziché all'Ietf, che tradizionalmente governa i protocolli Internet, è indicativo di una radicale contestazione, da parte della Cina, del modello multistakeholder di internet governance imposto dal governo statunitense dopo la privatizzazione della rete. Altrettanto radicale appare, sempre sul piano del codice informatico, il progetto della Federazione Russa di costruire un *Domain name system* (Dns) nazionale, in aperta contrapposizione con il Dns globale amministrato dalla *Internet corporation for assigned names and numbers* (Icann), perno dell'ordine neo-liberale digitale[14]. Sul piano giuridico internazionale, poi, i governi russo e cinese continuano a spingere, in sede Onu, in direzione di trattati intergovernativi per regolare alcune questioni relative alla rete o, in alcuni casi, il cyberspazio nel suo complesso. Alla prima categoria di trattati appartiene, ad esempio, la proposta russa discussa dall'Assemblea Generale delle Nazioni Uniti il 25 novembre 2019 tendente a un trattato internazionale sulla *cybersecurity*. Anche in questo caso, la proposta ha funzione di protesta. Nel campo della *cybersecurity*, infatti, esiste già una convenzione internazionale, la *Budapest convention on cybercrime*, elaborata dal Consiglio d'Europa nel 2001 ed entrata in vigore il primo luglio 2004. Una convenzione, però, non sottoscritta da Russia e Cina, che ritengono alcune disposizioni lesive della sovranità nazionale degli stati. La nuova iniziativa russa in tema di *cybersecurity* è stata avallata dall'Assemblea generale dell'Onu che, con 88 voti a favore, 58 contrari e 34 astenuti, ha deciso di istituire «un comitato intergovernativo di esperti per elaborare una convenzione internazionale sul contrasto all'uso delle tecnologie dell'informazione della comunicazione per fini criminali» (Un general assembly 2019). Alla categoria dei trattati internazionali che riguardano l'intero sistema della governance di internet appartengono invece due recenti istanze di consultazione presentate dalla Federazione Russa al quindicesimo meeting del *Council working group on international internet-related public policy issues* (Cwg-Internet) dell'Itu, svoltosi online il 27 gennaio 2021. In entrambe le proposte si attacca nuovamente il regime dei nomi di dominio e degli indirizzi di internet che ruota intorno ad Icann, e si invita gli Stati membri a «superare le sfide connesse alla dipendenza dalle decisioni di un'unica amministrazione nazionale, per continuare a costruire un sistema di internet governance indipendente, democratico ed equidistante da tutti gli

[14] Tale piano è stato sostanzialmente approvato con la cosiddetta Internet Sovereign Law, che in realtà consiste di tre emendamenti alle precedenti norme russe sulla comunicazione digitale introdotti dalla legge federale n. 90 del 1° maggio 2019. È interessante notare che, nel presentare la nuova normativa, la Duma sostenga che «il documento è stato preparato in considerazione della natura aggressiva della Strategia di Cybersecurity nazionale adottata dagli Stati Uniti nel settembre del 2018», Duma (2019), *Adozione della legge sul «Sovereign Internet»*, 14 aprile, duma.gov.ru/news/44551.

stati» (Itu 2021). Questo assalto, da est, alla costituzione del cyberspazio, ossia all'insieme di regole e principi codificati nei protocolli di base della rete e nei (pochi) trattati internazionali ad essa applicabili, rischia di trasformare la rete dalle fondamenta, alterando in maniera sostanziale i rapporti di forza tra gli attori della governance di internet, e con essi l'insieme di valori politici codificati nelle sue architetture.

4. Note conclusive

Il caso Solorigate testimonia di una crescente tensione internazionale tra, da un lato, il complesso militare-digitale statunitense e, dall'altro, le potenze tecnologiche emergenti di Russia e Cina. Entrambe le fazioni spingono in direzione di una militarizzazione del cyberspazio, con l'effetto, non secondario, di riportare al centro dell'ecosistema globale della governance di internet il ruolo degli stati nazionali e dei loro apparati di sicurezza. Esiste una terza via? Un recente contributo di Timothy Garton Ash, pubblicato da «la Repubblica», propone di esplorare nuove strade nell'ambito di quel «vertice delle democrazie» annunciato dal nuovo presidente Usa Joe Biden (Garton 2021). Garton Ash, d'altra parte, individua nelle grandi corporation del digitale il principale ostacolo a una democratizzazione atlantica della rete. In realtà, come abbiamo avuto modo di argomentare in questo insight, la sfida a una Internet democratica e pacifica non è posta solo da attori privati diventati eccessivamente potenti grazie a due decenni di *laissez-faire* cibernetico. Ma giunge anche dai governi degli stessi regimi democratici occidentali, che hanno ormai adottato un paradigma di *cybersecurity* fondato sulla compromissione della sicurezza delle reti. È dal superamento, per nulla scontato, di queste sfide che dipende la possibilità di un'alleanza delle democrazie per il cyberspazio che unisca la capacità americana di produrre codice informatico a quella europea di elaborare codice giuridico. L'Unione Europea, dopo decenni di immobilismo in questo campo, sta iniziando a fare la sua parte. Ne sono testimonianza la *General data protection regulation* (Gdpr), che opera, anche al di fuori dei confini europei, a tutela della privacy degli utenti delle reti, e le due recenti iniziative legislative della Commissione Europea note come *Digital services act* (Dsa) e *Digital markets act* (Dma), che mettono al centro della regolamentazione delle reti principi e valori democratici[15]. Lungo questa strada, come suggerito dal Presidente francese Emmanuel Macron nel suo discorso di apertura dell'Internet Governance Forum delle Nazioni Unite nel novembre del 2018, l'Unione Europea può candidarsi a guidare la costruzione di un nuovo

[15] Si veda European Commission (2020).

modello di Internet governance alternativo tanto al modello californiano quanto a quello cinese. Un modello basato sui diritti umani, più che sul diritto all'autodifesa degli stati o sul diritto umanitario internazionale. Un modello che, per essere effettivo e funzionante, necessita di una stagione politica di «costituzionalismo digitale», un termine coniato di recente da un network di studiosi, prevalentemente europei, per indicare l'urgenza e l'importanza di un processo di costituzionalizzazione del cyberspazio[16].

Riferimenti bibliografici

Braman, S. (2013), *The Geopolitical vs. the Network Political: Internet Designers and Governance*, in «International Journal of Media & Cultural Politics», 9 (3), pp. 277-296.

Bulfon, F. (2021), *Vaccini, firmati da hacker cinesi i raid all'Irbm di Pomezia. «Così si fingevano russi»*, la Repubblica, 30 gennaio, https://rep.repubblica.it/pwa/generale/2021/01/30/news/vaccino_astrazeneca_firmati_da_hacker_cinesi_i_raid_all_irbm_di_pomezia-285080938/.

Caralle, K. e Griffith, K. (2020), *Romney Warns Russian Cyber-attack Could 'Cripple' US Electricity and Water Supplies as he Condemns Trump for Refusing to Blame Putin and says Response Must be 'of Like Magnitude or Greater'*, Daily Mail, 20 dicembre, https://www.dailymail.co.uk/news/article-9072851/Mitt-Romney-condemns-Trumps-refusal-accept-U-S-intelligence-blame-Kremlin-cyber-attack.html.

Cisa (2020), Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*, 13 dicembre, https://cyber.dhs.gov/ed/21-01/.

Cohen, Z. e Marquardt, A. (2020), *CIA Cyber Weapons Stolen in Historic Breach Due to 'Woefully Lax Security', Internal Report Says*, CNN, 16 giugno, https://edition.cnn.com/2020/06/16/politics/cia-wikileaks-vault-7-leak-report/index.html.

De Groot, G.J. (2006), *Dark Side of the Moon. The Magnificent Madness of the American Lunar Quest,* New York e London, New York University Press.

Dilanian, K., Lederman, J., Stelloh T. e Collier, K. (2020), *Russian Hackers Breach U.S. Government, Targeting Agencies, Private Companies*, NBC News, 14 dicembre, https://www.nbcnews.com/news/us-news/russian-hackers-breach-u-s-government-effort-aimed-agencies-private-n1251057.

European Commission (2020), *The Digital Services Act package*, 15 dicembre, https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

Fraser, B. (1997), *Request for Comments: 1244, Site Security Handbook*, settembre 1997, https://tools.ietf.org/html/rfc2196. Consultato il 10 febbraio 2021.

[16] Digital Constitutionalism Network (https://digitalconstitutionalism.org.).

Gallagher, R. (2020), *SolarWinds Adviser Warned of Lax Security Years Before Hack*, Bloomberg, 21 dicembre, https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack.

Garton, T.A. (2021), *Biden nell'arena digitale*, la Repubblica, 10 febbraio, https://rep.repubblica.it/pwa/commento/2021/02/09/news/stati_uniti_joe_biden_europa_democrazia_digitale-286795468/.

Internet Activities Board (1989), *Request for Comments: 1087, Ethics and the Internet*, gennaio 1989, https://tools.ietf.org/html/rfc1087. Consultato il 10 febbraio 2021.

Itu (2021), *Report of the Fifteenth Meeting of the Council Working Group on International Internet-related Public Policy Issues (CWG-Internet)*, 28 gennaio, https://www.itu.int/md/S21-RCLINTPOL15-C-0012/en. Consultato il 10 febbraio 2021.

Holbrook, J.P. e Reynolds, J.K. (1991), *Request for Comments: 1244, Site Security Handbook*, luglio 1991, https://tools.ietf.org/html/rfc1244. Consultato il 10 febbraio 2021.

Lenthang, M. (2021), *SolarWinds Cybersecurity Expert Warned Management in 2017 about Risk of 'Catastrophic' Breach - As It's Revealed Cost-saving Move to Eastern Europe Could Have Exposed Firm to Major Russian Hack*, Daily Mail, 3 gennaio, https://www.dailymail.co.uk/news/article-9108511/SolarWinds-warned-potential-cyber-attack-cost-saving-Europe-exposed-firm.html.

Mandia, K. (2020), *FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community*, FireEye, 8 dicembre, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.

Nakashima, E. e Timberg, C. (2020), *Russian Government Hackers are Behind a Broad Espionage Campaign that Has Compromised U.S. Agencies, Including Treasury and Commerce*, The Washington Post, 14 dicembre, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

Perlroth, N. (2021), *How the United States Lost to Hackers*, The New York Times, 6 febbraio, https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html.

Sanger, D.E. e Perlroth, N. (2020), *FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State*, The New York Times, 8 dicembre https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html.

Sanger, D.E., Perlroth, N. e Barnes, J.E. (2021), *As Understanding of Russian Hacking Grows, So Does Alarm*, The New York Times, 2 gennaio, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Sanger, D., Perlroth, N. e Shane, S. (2019), *How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks*, The New York Times, 6 maggio, https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

Schmitt, M.N. (2013), *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge, Cambridge University Press.

SolarWinds Corporation (2020), *Current Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934*, 14 dicembre, https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm.

Stone, A. (2019), *How Leon Panetta's 'Cyber Pearl Harbor' warning shaped Cyber Command*, Fifth Domain, 30 luglio, https://www.fifthdomain.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command.

Tonacci, F. (2020)*, Piero Di Lorenzo: Attaccati dagli hacker, così hanno cercato di ritardare la corsa di AstraZeneca*, la Repubblica, 3 dicembre, https://rep.repubblica.it/pwa/intervista/2020/12/03/news/attaccati_dagli_hacker_cosi_hanno_cercato_di_ritardare_la_corsa_di_astrazeneca_-276928378/.

UN General Assembly (2019), *Countering the Use of Information and Communications Technologies for Criminal Purposes*, 25 novembre, https://www.undocs.org/A/74/401. Consultato il 20 gennaio 2021.

UK National Cyber Security Centre (NCSC) (2020), *Advisory: APT29 Targets COVID-19 Vaccine Development,* 16 luglio, consultato il 10 febbraio 2021.

Zorloni, L. (2020), *La Cina vuole cambiare le regole di internet, ma non ci è riuscita. Per ora*, Wired, 22 dicembre, https://www.wired.it/internet/web/2020/12/22/cina-internet-new-ip-itu-consenso.