Cercasi vincitori del Premio Nobel per la Pace che creino la pace nel cyberspazio

Wolfgang Kleinwächter

Traduzione a cura di Adriana Lazzaroni, IIT- CNR

Il 1° gennaio 2022 la Germania ha assunto la presidenza del G7. In cima all'agenda, oltre al cambiamento climatico e alla crisi del Coronavirus, c'è la sicurezza informatica, il che è logico dal momento che la pandemia in particolare ha dimostrato quanto il nostro mondo sia diventato dipendente da un'infrastruttura digitale sicura. L'instabilità del cyberspazio rappresenta una minaccia per le future generazioni tanto quanto un ambiente distrutto.

Negli ultimi due decenni quasi nulla è cambiato di più del mondo di Internet. Nato come una promessa di libertà e di crescita, Internet oggi è visto sempre più come un fattore di rischio. La comunicazione senza confini e l'innovazione infinita sono state oscurate dalla corsa agli armamenti digitali, dallo spionaggio informatico e dagli attacchi ransomware. Su Internet, tutto sembra essere il contrario di tutto. Libertà e prosperità per alcuni, sorveglianza e sfruttamento orwelliano per altri. Internet offre a sviluppatori creativi, imprenditori innovativi e cittadini responsabili le stesse opportunità che mette a disposizione di predicatori di odio, pedofili e guerrafondai. E non è ancora chiaro chi avrà la meglio in questa lotta appena scoppiata tra "bene" e "male". Se oggi dovesse scoppiare una "vera guerra" - ha recentemente affermato il Presidente degli Stati Uniti Joe Biden - probabilmente inizierebbe con un attacco informatico.

In questo senso, è più che giustificato fare della costruzione di un'architettura globale di sicurezza informatica una priorità della diplomazia nell'era digitale. Gli Stati Uniti e la Cina si stanno dirigendo verso una guerra fredda informatica. Gli attacchi digitali alle infrastrutture critiche stanno proliferando. I droni intelligenti, programmati con software di riconoscimento facciale, cercano i propri obiettivi da uccidere. Cosa si può fare?

La buona notizia è che i governi e gli attori non statali parlano da anni dei rischi e degli effetti collaterali dell'era dell'informazione. Nel 2005 si è tenuto a Tunisi il Vertice mondiale delle Nazioni Unite sulla Società dell'Informazione (*World Summit on the Information Society*, WSIS). In quell'occasione è stata adottata un'"Agenda" con linee guida per un futuro digitale pacifico e aperto, incentrato sulle persone. Da allora si è tenuto l'"Internet Governance Forum" (IGF), il "summit digitale" annuale delle Nazioni Unite. La prossima conferenza di revisione del WSIS è prevista per il 2025. Inoltre, sotto l'egida delle Nazioni Unite, si sono costituiti altri organismi per affrontare i temi della sicurezza informatica, dell'economia digitale e dei diritti umani nello spazio virtuale. Il mondo sa quindi quali pericoli si nascondono nel cyberspazio e cosa si dovrebbe fare.

La cattiva notizia, però, è che finora non è stato concordato praticamente nulla di concreto. Esiste ancora un divario digitale, nonostante i progressi compiuti negli ultimi anni nello sviluppo delle infrastrutture informatiche, con quasi cinque miliardi di utenti di Internet nel 2022. Nel cyberspazio avvengono massicce violazioni dei diritti umani, con una crescente censura e sorveglianza di massa. Ci sono nuovi oligopoli nell'economia digitale che ostacolano la concorrenza leale e l'innovazione. Il flusso di dati transfrontaliero diventa parte di una guerra commerciale digitale. Gli attacchi informatici da parte di attori statali e non statali minano la pace globale e la sicurezza internazionale.

20 anni fa, il WSIS era l'unica piattaforma intergovernativa che si occupava delle questioni di *public policies* legate a Internet. Oggi esistono numerose piattaforme negoziali in cui i governi, le imprese, la società civile e la comunità tecnica cercano di trovare soluzioni per le questioni emerse nell'ecosistema globale della governance di Internet dal 2005, quando l'"Agenda di Tunisi" è stata adottata da 193 capi

di Stato. L'UNESCO si occupa di intelligenza artificiale. L'ITU si occupa dello sviluppo di un'infrastruttura digitale, WTO del commercio digitale, ILO delle conseguenze della digitalizzazione sul mercato del lavoro. Il Consiglio per i diritti umani delle Nazioni Unite (UNHRC) sta discutendo su come i diritti umani debbano essere implementati nel mondo online. Sulla base delle raccomandazioni provenienti dal gruppo di lavoro delle Nazioni Unite "High Level Panel on Digital Cooperation", presieduto da Jack Ma di AliBaba e da Melinda Gates della Microsoft Foundation, il Segretario Generale delle Nazioni Unite Antonio Guterres ha pubblicato un rapporto per la cooperazione digitale denominato “Roadmap for Digital Cooperation” nel giugno 2020 e ha ora proposto un "Global Digital Compact" che potrebbe guidare il mondo verso il 2030.

Tuttavia, tutti i negoziati non hanno prodotto accordi concreti con impegni chiari. Ci sono numerosi rapporti e documenti di base sui vari tavoli delle conferenze, ma non c'è alcun accordo. Alcuni organismi delle Nazioni Unite - OEWG, AHC, LAWS - stanno negoziando la sicurezza nel cyberspazio, ma in tutti e tre i gruppi le controversie sono maggiori della volontà di raggiungere un accordo su un progetto comune.

Comportamento degli Stati nel cyberspazio

Diamo uno sguardo più approfondito ai negoziati sulla sicurezza informatica a livello mondiale. La cybersecurity è oggi un problema centrale della sicurezza nazionale e internazionale. E il numero di attacchi nel cyberspazio è in crescita.

La prima piattaforma negoziale è l'Open Ended Working Group (OEWG). L'OEWG è stato istituito nel 2018 nell'ambito del 1° Comitato dell'Assemblea Generale delle Nazioni Unite. Si è basato sul lavoro di diversi cosiddetti "Gruppi di esperti governativi" (*Group of Governmental Experts*, GGE) che dal 2004 hanno lavorato sulle norme di comportamento degli Stati nel cyberspazio. Il GGE è riuscito a trovare un accordo su undici norme - tra cui quella di non attaccare le infrastrutture cibernetiche di altri Paesi - e su una serie di misure di rafforzamento della fiducia. Ha inoltre convenuto che il diritto internazionale e la Carta delle Nazioni Unite sono rilevanti sia offline che online. Nel 2020 il mandato dell'OEWG è stato esteso al 2025. Tutti i 193 Stati membri delle Nazioni Unite partecipano ai suoi lavori. Il suo compito è quello di chiarire cosa costituisce un comportamento corretto da parte degli Stati nel cyberspazio, in conformità con il diritto internazionale. Sulla base dell'accordo che il diritto internazionale si applica non solo al mondo analogico, ma anche a quello digitale, quello dell’OEWG non dovrebbe essere un compito complicato. Non è necessario reinventare la ruota o scrivere una nuova Carta delle Nazioni Unite. Ma le controversie iniziano quando le cose si fanno concrete. Quand’è che un "attacco informatico" costituisce un uso della forza contrario al diritto internazionale ai sensi dell'articolo 2, paragrafo 4, della Carta delle Nazioni Unite e fa scattare il diritto all'autodifesa, sancito dall'articolo 51? Può un "hack-back" essere giustificato dall'articolo 51 che prevede il diritto all'autodifesa? Oppure si può rispondere asimmetricamente a un attacco informatico con un bombardamento, come ha fatto Israele a Gaza dopo un attacco informatico di Hamas? Il problema è che non solo c'è disaccordo su cosa costituisca esattamente un attacco informatico, ma anche l'aggressore è in molti casi difficile da determinare. Se un carro armato attraversa il confine, tutti sanno da dove proviene. Ma se un malware viene installato in una centrale elettrica e si attiva solo dopo sei mesi, non è facile per lo Stato attaccato dimostrare al cento per cento la provenienza dell'attacco.

Pertanto, l'OEWG si occupa anche del ruolo degli attori non statali e delle misure di rafforzamento della fiducia e di *capacity building*. Idee come la creazione di un punto di contatto permanente per le situazioni di crisi o l'organizzazione di una più stretta collaborazione tra esperti tecnici e diplomatici sono passi ragionevoli. La prima riunione dell'OEWG, tenutasi a New York all'inizio di dicembre 2021, si è svolta in un'atmosfera assolutamente costruttiva, ma non è stato possibile trovare un accordo su come gli attori non governativi saranno coinvolti nei futuri negoziati. Inoltre, non è chiaro cosa

dovrebbe effettivamente emergere dai negoziati: un piano d'azione? Un codice di condotta? Un patto di non aggressione informatica?

Criminalità informatica

La seconda piattaforma negoziale riguarda l'esplosione della criminalità nel cyberspazio. Per la criminalità organizzata, lo spazio virtuale è diventato più redditizio del traffico di droga o di esseri umani. Esiste già un trattato internazionale contro la criminalità informatica: la Convenzione di Budapest, firmata nel novembre 2001, poche settimane dopo gli attacchi terroristici al World Trade Center di New York dell'11 settembre.

Questo trattato è stato redatto sotto l'egida del Consiglio d'Europa ed è aperto alla firma di tutti i Paesi. I Paesi occidentali si sono a lungo battuti per l'universalizzazione della Convenzione di Budapest, ma solo un terzo dei 193 Paesi delle Nazioni Unite l'ha firmata. I principali Paesi digitalizzati, come India, Brasile e Cina, non hanno partecipato ai negoziati e hanno sostenuto la proposta russa di redigere una nuova convenzione ONU.

La preoccupazione dei Paesi occidentali è che i nuovi negoziati possano minare le norme già in vigore e abbassare lo standard abbastanza efficace della Convenzione di Budapest. Si prevedono controversie soprattutto per quanto riguarda la criminalizzazione dei contenuti informativi. Come possono democrazie e autocrazie accordarsi su quali espressioni di opinioni sono consentite su Internet?

Il piano prevede che la nuova Convenzione ONU in materia di Cybercrime sia pronta entro la fine del 2023. Si tratta di un calendario difficile, ma non del tutto irrealistico. Innanzitutto, molti passaggi della Convenzione di Budapest possono essere facilmente adottati. In secondo luogo, la pressione della sofferenza generata dalla mafia informatica globale, con le sue estorsioni a ospedali e amministrazioni pubbliche e gli attacchi alle catene di approvvigionamento globali e alle infrastrutture critiche, è ora equamente distribuita al di là dei confini ideologici. Se i negoziatori del nuovo Comitato Ad Hoc (*Ad Hoc Committee*, AHC) si concentreranno su ciò che è fattibile, i progressi non saranno impossibili.

Sistemi d'arma autonomi

La terza piattaforma negoziale riguarda i sistemi d'arma autonomi. Qui, nell'ambito della Convenzione sulle armi convenzionali (*Convention on Conventional Weapons*, CCW), un gruppo di esperti sotto l'acronimo LAWS (*Lethal Autonomous Weapon Systems*) sta negoziando su robot e droni killer dal 2014. Il Segretario Generale delle Nazioni Unite Antonio Guterres chiede da anni la messa al bando delle armi autonome, ma un gruppo molto eterogeneo di Stati - Russia, Cina, Stati Uniti, Israele, Turchia - ha finora rifiutato persino una moratoria. Naturalmente vi è un accordo di fondo per non lasciare che un algoritmo prenda decisioni di vita o di morte. Ma le opinioni divergono anche sulla definizione di ciò che costituisce un sistema d'arma autonomo. E mentre l'ostruzionismo continua a Ginevra, l'uso di droni armati nelle guerre locali sta diventando una pratica comune, come in Nagorno-Karabakh, Yemen, Libia, Medio Oriente, Ucraina e altrove. Il problema è complicato. Si possono concordare limiti massimi per le testate nucleari, ma qual è il limite per un algoritmo? Carri armati e aerei possono essere contati e controllati, ma come si fa a contare e verificare bit e byte?

Quando si tratta di sistemi d'arma autonomi, i tradizionali rituali dei negoziati sul disarmo stanno raggiungendo i loro limiti. Sono più che mai necessari la volontà politica degli attori coinvolti e un minimo di fiducia. E questo dipende in gran parte dalla misura in cui si riconosce come potrebbe svolgersi una guerra con armi digitali. Il Segretario Generale della NATO, Jens Stoltenberg, ha recentemente ricordato il periodo precedente alla Prima Guerra Mondiale. Non solo il mondo era "scivolato" in una guerra mondiale nel 1914, ha detto, ma i leader politici dell'epoca avevano completamente sottovalutato gli effetti delle nuove tecnologie dell'epoca, dai bombardieri e dai carri

armati ai gas asfissianti. Franz Haber, che in seguito vinse il Premio Nobel per la Chimica e fu coinvolto nello sviluppo del gas cloro all'inizio degli anni dieci, convinse i politici che l'uso di quest'arma avrebbe contribuito a porre rapidamente fine alla guerra. Ma si sbagliava. Fu vero il contrario. Milioni di persone morirono e le armi chimiche divennero un'altra fonte di instabilità nel nostro fragile mondo. Cosa accadrebbe se il vaso di Pandora dei sistemi d'arma autonomi venisse aperto in un conflitto odierno?

Standard tecnici di Internet

C'è poi una quarta piattaforma negoziale: la protezione del *public core* di Internet. Il funzionamento dell'infrastruttura di Internet e la disponibilità delle risorse corrispondenti - root server, nomi a dominio, indirizzi IP, protocolli Internet - hanno ormai la stessa elementare importanza delle forniture di acqua ed elettricità. Queste risorse sono gestite da diverse organizzazioni tecniche – ICANN (Internet Corporation for Assigned Names and Numbers), IETF (Internet Engineering Task Force), RIRs (Regional Internet Registries). Nel 2016, dopo che il governo degli Stati Uniti - sotto l'amministrazione Obama - ha trasferito la sua storica supervisione della root server A di Internet ad ICANN, ci sono stati ripetuti dubbi, soprattutto da parte di Cina e Russia, sulla capacità di questa comunità tecnica di gestire le risorse tecniche nell'interesse della comunità globale.

Ma non si è verificato nessun disastro. Al contrario, se c'era bisogno di uno stress test della resilienza del sistema, che funziona da più di 20 anni, la pandemia ne ha fornito la prova. Dopo l'epidemia di Coronavirus, c'è stata una crescita esorbitante dell'uso di Internet. Lo smart working, le teleconferenze, lo shopping online, l'apprendimento a distanza hanno fatto esplodere la domanda di nomi a dominio e di indirizzi IP. Il sistema esistente è stato in grado di gestire queste nuove sfide senza problemi. Non c'era carenza di indirizzi IP o di nomi di dominio e la root e i nameserver funzionavano.

Se queste risorse tecniche venissero coinvolte in un gioco di potere geostrategico, i rischi sarebbero notevoli. Così come non esiste aria cinese o americana, ma solo aria pulita o inquinata, le risorse tecniche di Internet sono politicamente neutrali. Se diventassero oggetto di un braccio di ferro politico, tutti ne subirebbero le conseguenze. È stato quindi molto sensato che sotto la presidenza britannica del G7 i ministri del digitale si siano chiaramente impegnati a lasciare l'elaborazione degli standard tecnici digitali nelle mani della comunità tecnica. La Presidenza tedesca del G7 dovrebbe continuare a perseguire questa strada con vigore.

Una doppia strategia per il cyberspazio

Il nuovo governo tedesco, nel suo ruolo di presidente del G7 nel 2022, deve affrontare un'ampia gamma di sfide sul fronte digitale. Il mondo ha più che mai bisogno di un multilateralismo sostenibile ed equo per il cyberspazio, che sia guidato dai valori universali della Carta delle Nazioni Unite e della Dichiarazione dei diritti umani dell'ONU, e che si fondi su una stretta collaborazione tra governi, imprese, società civile e comunità tecnica. Con la presidenza del G7, molti occhi sono ora puntati sulla Germania, che ha ospitato l'Internet Governance Forum delle Nazioni Unite nel 2019, e ciò si ripercuoterà anche nei negoziati sui sistemi d'arma autonomi. Nel gennaio 2020, la deputata dei Verdi al Bundestag, Katja Keul, aveva criticato l'allora governo tedesco per non aver sostenuto con sufficiente forza il divieto di queste armi nel diritto internazionale. L'accordo di coalizione prevede ora che il nuovo governo federale prenda iniziative tempestive sul controllo degli armamenti nell'ambiente cyber e dell'intelligenza artificiale. La sezione tedesca dell'organizzazione non governativa "Stop Killer Robots" ha criticato questa decisione definendola troppo morbida. Anche l'UE non ha ancora preso posizione. Katja Keul è ora Segretario di Stato presso il Ministero degli Esteri tedesco. Si tratta di un compito entusiasmante in cui si può anche imparare dall'esperienza storica.

All'inizio di dicembre 2021, la Fondazione Friedrich Ebert ha tenuto una conferenza per celebrare il 50° anniversario dell'assegnazione del Premio Nobel per la Pace a Willy Brandt. Essa ha saggiamente

elaborato che la Ostpolitik di Brandt si basava su una duplice strategia. Il concetto di "cambiamento attraverso il riavvicinamento" consisteva sia nel tendere la mano al rivale del sistema sia nel rafforzare le risorse del Paese. Il *Rapporto Harmel* della NATO del 1967, al quale Brandt aveva partecipato come ministro degli Esteri dell'allora Grande Coalizione, costituì la base per la creazione di una rete di "trattati di distensione" - dai trattati bilaterali tra Germania Ovest e Unione Sovietica, tra Polonia e Cecoslovacchia, passando per l'Accordo di Berlino (1971), gli Accordi Sovietico-Statunitensi-SALT fino all'Atto Finale di Helsinki (1975) - che assicurarono la pace, almeno per l'Europa, per diversi decenni. I trattati degli anni '70 non si basavano sul fatto che i diversi sistemi sociali fossero da considerarsi buoni. In questo caso, le persone erano d'accordo sul fatto di non essere d'accordo, ma vi era un interesse prioritario a rinunciare alla violenza e a proteggere il patrimonio comune dell'umanità, che includeva gli interessi legittimi dell'altra parte. La sicurezza era intesa come sicurezza collettiva con il sistema rivale, non contro di esso.

Joseph Nye, decano di Scienze politiche americane, ci ha ricordato nel saggio "*The End of Cyber-Anarchy*", nel numero di gennaio 2022 della rivista *Foreign Affairs*, che nella Guerra Fredda le escalation temporanee delle crisi e i negoziati sui trattati di stabilizzazione erano due facce della stessa medaglia. I disaccordi concettuali sul futuro del mondo digitale non dovrebbero essere un ostacolo ad un accordo selettivo sulla stabilità nel cyberspazio. Anche Wolfgang Ischinger, ex capo della Conferenza sulla Sicurezza di Monaco, vede nella riattivazione dei principi dell'Atto finale della Conferenza sulla sicurezza e la cooperazione in Europa (CSCE) del 1975 e della Carta di Parigi del 1992 una strategia sensata per contrastare le nuove minacce del 2020.

La proposta del Segretario Generale delle Nazioni Unite, Antonio Guterres, di utilizzare il Vertice sul futuro delle Nazioni Unite, previsto per il 2023, per adottare un "Patto Digitale Globale" potrebbe divenire un importante tassello per una nuova architettura di cybersecurity. L'idea del Presidente finlandese, Sauli Niinistö, di utilizzare il 50° anniversario dell'Atto finale di Helsinki nel 2025 per promuovere la sicurezza nel cyberspazio potrebbe essere un buon inizio. In ogni caso, se qualcuno troverà il codice per una pace informatica duratura, lei o lui sarà un buon candidato per il prossimo Premio Nobel per la Pace.