Human Security

N. 07

Luglio 2018

Dimensioni e prospettive dei conflitti contemporanei

Cybersecurity - Human Security.

di ***Giampiero Giacomello***

Computer e reti informatiche sono così pervasivi e onnipresenti che solo raramente ci si sofferma a riflettere su quanto essi abbiano trasformato la società e l'economia mondiale. Un comune smartphone di oggi ha una capacità di calcolo molto superiore a quella di un computer portatile di soli dieci anni fa, e cambiamenti simili sono avvenuti in ogni settore tecnologico. Una maggiore attenzione alla sicurezza dello spazio cibernetico – la *cybersecurity* – è oggi essenziale. Non sorprende dunque che la domanda di "esperti in *cybersecurity*" sia in continua crescita e che la sicurezza in ambito cibernetico sia ormai uno dei temi di ricerca di maggior interesse nei cosiddetti *security studies*. Ma che cosa si intende esattamente per *cybersecurity*?

La domanda è più che legittima, dato che non esiste una definizione universalmente condivisa di *cybersecurity*. Proprio come i computer e le reti sono presenti in ogni segmento delle società avanzate, così la sicurezza dello spazio cibernetico riguarda tanto i software (codici e programmi) e gli hardware (*router* e macchine) quanto gli utilizzatori degli stessi (persone) – in altre parole, *tutto*.

Lo spazio cibernetico, o cyberspazio, è a sua volta composto di vari livelli: (a) un livello fisico, fatto di cavi, fibre ottiche, *router* e *switches*; (b) un livello logico di codici e software che consentono a macchine diverse, con diversi sistemi operativi, di dialogare fra loro senza soluzione di continuità; e infine (c) un livello sociale o semantico, che è quello degli utilizzatori umani, non necessariamente esperti di informatica e tecnologia. Come si può facilmente immaginare, ciascuno di questi livelli è soggetto a potenziali malfunzionamenti.

Rotture e incidenti sono propri di qualsiasi sistema – e anzi più un sistema è complesso, più è incline a errori. Nel caso del cyberspazio, inoltre, pochi degli elementi fondamentali sono stati sviluppati e creati pensando alla sicurezza degli stessi, dato che, in origine, l'idea degli ingegneri informatici era quella di massimizzare l'efficienza della comunicazione e dello scambio delle informazioni. L'obiettivo non è cambiato, ma governi, sviluppatori e utenti si sono accorti, loro malgrado, che le "imperfezioni" del sistema rappresentano vulnerabilità che alcuni attori – come governi, gruppi criminali o addirittura adolescenti annoiati (ma tecnicamente capaci) – possono sfruttare per profitto, fini politici o semplicemente

Nel 2010, gli utenti di internet erano meno di 2 miliardi. Oggi, circa metà della popolazione mondiale è online e la crescita è rapida, soprattutto nei paesi in via di sviluppo. I nuovi prodotti e servizi di cui disponiamo stanno però facendo molto di più che fornire nuove possibilità: stanno cambiando il nostro modo di vivere, lavorare e relazionarci gli uni con gli altri.

Dai robot alle auto a guida autonoma, quella che fino a qualche anno fa sembrava solo fantascienza è oggi diventata realtà. Se è vero che l'intelligenza artificiale potrebbe migliorare notevolmente le nostre vite, è anche vero, però, che tutte le tecnologie possono essere utilizzate sia per contribuire al progresso umano che per servire obiettivi meno nobili, se non addirittura criminali. Il settimo numero di ***Human Security*** è quindi dedicato ad alcuni degli aspetti più critici della cosiddetta Quarta rivoluzione industriale e, in particolare, alla trasformazione tecnologica del conflitto e della sicurezza.

Ciò che vale per la sfera privata o per il settore industriale, infatti, vale anche per la guerra. Come sempre più spesso si legge sui giornali, i conflitti contemporanei non si limitano più ai tradizionali campi di battaglia – suolo, mare e aria – ma sembrano aver varcato la soglia di una nuova arena, potenzialmente sconfinata: lo spazio cibernetico. Non sorprende, quindi, il crescente interesse e la sempre maggiore attenzione alla ***cybersecurity***. Giampiero Giacomello, docente di scienza politica all'Università di Bologna, sottolinea quanto l'uso di nuove tecnologie in settori sensibili come la finanza, l'assistenza sanitaria, le telecomunicazioni e i trasporti porti con sé nuovi rischi ed esponga governi e cittadini a "guerre con il computer" che possono colpire chiunque, dovunque e in qualsiasi momento.

Tra le tante sfide che il mondo deve affrontare, quella forse più intensa è capire quale sarà l'evoluzione del rapporto uomo-macchina in ambito bellico: è possibile delegare ai robot l'attività che da sempre ci distingue da tutti gli altri esseri viventi? Nel suo articolo, Christopher Coker, docente di relazioni internazionali alla London School of Economics and Political Science, approfondisce il tema, basando il proprio ragionamento sulle differenze fondamentali fra **intelligenza artificiale** e intelligenza umana.

Al di là delle possibili traiettorie future, l'impiego di armi in grado di agire autonomamente dall'intervento umano è realtà in diversi contesti di conflitto già da molti anni. Nonostante ciò, l'unico tentativo concreto di regolamentarne l'uso rimane quello di Isaac Asimov, che nel 1950 elaborò le tre leggi della robotica. Affrontando il tema da una prospettiva giuridica, Andrea Spagnolo, docente di Diritto internazionale umanitario presso l'Università di Torino, analizza il dibattito scaturito dal lavoro del Gruppo di esperti sulle armi autonome nell'ambito della *Convention on Certain Conventional Weapons* (CCW) ed evidenzia come la mancata ***regolamentazione delle armi autonome*** possa compromettere il rispetto dei principi cardine del diritto umanitario stabiliti dalle Convenzioni di Ginevra.

Se nel 1949 gli stati hanno riconosciuto la necessità di aderire a regole che proteggano i civili in tempo di guerra, Pier Luigi Dal Pino, direttore centrale delle relazioni istituzionali e industriali di Microsoft Italia e Austria, sottolinea la necessità di una *Digital Geneva Convention* che protegga i civili nel cyberspazio anche in tempo di pace. Descrivendo il ruolo fondamentale e l'impegno del settore privato nella prevenzione e nella gestione degli attacchi informatici, Dal Pino introduce il ***Cybersecurity Tech Accord***, siglato recentemente dalle principali imprese informatiche, ed incoraggia i governi a fare altrettanto.

Chiude questo numero di *Human Security* un articolo a firma di Gioachino Panzieri, neolaureato presso l'Università di Torino, che guarda all'uso della tecnologia e in particolare all'**attivismo digitale** come strumento di analisi capace di catturare la complessità dei conflitti contemporanei a partire "dal basso" e quindi in grado di restituire un ruolo di primo piano alla popolazione locale e alla *digital community* a cui si l'informazione si rivolge.

twai TORINO WORLD AFFAIRS INSTITUTE

Human Security è sostenuto da:

Compagnia di San Paolo

International Affairs

ISSN 2531-4998

grafica e impaginazione: www.glamlab.it

visibilità e notorietà. Ecco che la stabilità e la sicurezza del cyberspazio diventano obiettivi cruciali.

Data la complessità e vastità della materia, in questo breve articolo ci limiteremo a illustrare due dei temi più rilevanti nell'ambito della *cybersecurity*: la protezione delle infrastrutture critiche e la *cyberwar* o *cyberwarfare*, cioè, semplificando, la "guerra con il computer" che può colpire chiunque, dovunque e in qualsiasi momento.

Le infrastrutture critiche si potrebbe dire siano il sistema nervoso o linfatico delle società contemporanee e dell'economia moderna: non solo esse consentono alle informazioni di circolare, ma "trasportano" anche materie prime e servizi. In generale, e nonostante alcune differenze, molti paesi avanzati considerano i seguenti settori parte delle proprie infrastrutture critiche: banche e finanza, amministrazione pubblica, telecomunicazioni, distribuzione di acqua, gas ed energia, trasporti (tutti), servizi ospedalieri e di emergenza. Come è facile immaginare, se qualcuno tra questi settori dovesse cessare di funzionare per un periodo più o meno lungo, la vita dei cittadini e il normale funzionamento dei paesi ne sarebbero sostanzialmente intaccati. Inoltre, alcuni di questi settori provocano "effetti a cascata", amplificando il danno: se cessa la distribuzione di energia elettrica, ad esempio, tutto il resto si ferma di pari passo, mentre se questo accadesse per i trasporti, si interromperebbero di conseguenza i servizi ospedalieri e di distribuzione alimentare, con effetti drammatici che non è difficile immaginare.

In passato, le infrastrutture critiche erano prevalentemente fisiche, oggi sono tutte fisico-digitali. A metà degli anni Novanta, infatti, quando internet divenne "pubblica" per gentile concessione del governo americano, molte aziende scoprirono non solo i vantaggi delle comunicazioni digitali, ma anche la possibilità di "monitorare in remoto" molte delle loro strutture e filiali. Ad esempio, una stazione di monitoraggio di una condotta del gas, magari collocata in un'area remota, richiedeva in origine che un addetto si spostasse fisicamente fino a tale stazione, leggesse i dati e li riportasse alla centrale. La gestione in remoto consente evidentemente di abbattere i costi e di risparmiare tempo. Che il settore privato si adeguasse in toto a queste innovazioni non può quindi sorprendere; tuttavia anche i servizi pubblici, costretti ad adeguarsi alle stesse condizioni di efficienza del settore privato, ne hanno seguito l'esempio.

Come già anticipato, però, la progettazione dei protocolli e dei sistemi di comunicazione tra reti e computer, basata sulla massimizzazione dell'efficienza nello scambio di informazioni, ha aumentato il rischio che qualcuno potesse sfruttarne le debolezze per provocare danni e interruzioni: è oggi sufficiente la manomissione della sola componente digitale di un'infrastruttura critica per alterarne anche il funzionamento fisico. Considerando che, da sempre, le infrastrutture critiche sono un obiettivo strategico in un contesto di conflitto armato, è evidente come la possibilità di colpirle tramite attacchi informatici rappresenti un notevole vantaggio per l'aggressore.

Fonte: Symantec ISTR/NCIRC NATO.

Una banca attaccata da un gruppo criminale può perdere denaro e reputazione, e a soffrirne saranno soprattutto i suoi clienti; se invece lo stesso gruppo criminale interrompesse la fornitura elettrica o del gas in inverno per un periodo prolungato, le conseguenze ricadrebbero su gran parte della popolazione. Se quanto è successo l'anno scorso nel Regno Unito con l'attacco *ransomware* "WannaCry" (responsabile di un'epidemia informatica su larga scala che ha reso inaccessibili, fra l'altro, le cartelle cliniche dei pazienti di numerosi ospedali) fosse durato alcune settimane invece di qualche giorno, le conseguenze sarebbero state ben più severe e diffuse. Tutto questo è noto

Autori

Giampiero Giacomello, *docente di Scienza Politica, Università di Bologna*

Christopher Coker, *docente di International Relations, London School of Economics and Political Science*

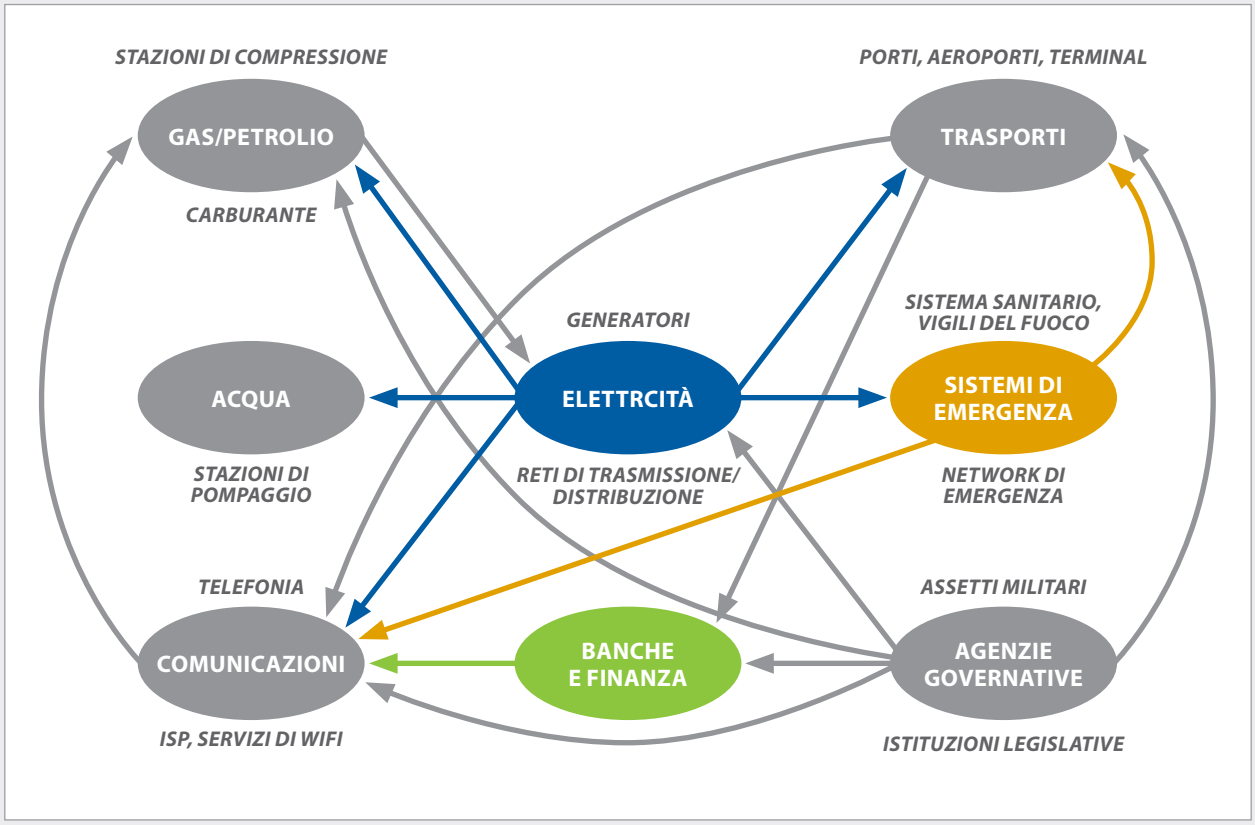
Andrea Spagnolo, *docente di Diritto Internazionale Umanitario, Università di Torino*

Pier Luigi Dal Pino, *direttore centrale delle relazioni istituzionali e industriali, Microsoft Italia e Austria*

Gioachino Panzieri, *neolaureato in Cooperazione Internazionale allo Sviluppo, Università di Torino*

humansecurity@twai.it

Le infrastrutture critiche sono interdipendenti.



agli *hacker black-hat* (i "cattivi", contrapposti ai *white-hat*), al crimine organizzato ("WannaCry" aveva scopo di estorsione, ad esempio) e, non da ultimo, ai governi di molti paesi.

Anche *cyberwar* e *cyberwarfare* sono termini diventati popolari quanto '*cyberspace*'. Essenzialmente, si riferiscono all'impiego delle *Information Technologies* (IT) – nella loro accezione più estesa – nella condotta di operazioni militari o, in altre parole, alla proiezione delle tecniche belliche nello spazio cibernetico, che è diventato a tutti gli effetti uno degli ambiti operativi della NATO, proprio come lo spazio o gli oceani. La NATO fa riferimento alle *Computer Network Operations* (CNO), tradizionali compiti militari di attacco e difesa, e alle *Computer Network Exploitations* (CNE), che riguardano ad esempio sabotaggio e spionaggio. In questo ambito, la distinzione fra dimensione "civile" e "militare" è però tutt'altro che agevole: le tecniche utilizzate per le CNO e per le CNE sono pressoché le stesse ed è dunque difficile stabilire se una penetrazione della rete informatica militare da parte di un potenziale avversario è il preludio di un attacco convenzionale ("cinetico"), una semplice attività di spionaggio oppure un tentativo di sabotaggio a lungo termine. Se comprendere la finalità ultima di un *cyberattack* è già di per sé un problema (un missile lanciato contro un bersaglio è certo meno ambiguo), anche l'attribuzione di responsabilità dell'atto è una questione complessa e delicata. L'aggressore infatti cercherà sempre di coprire il più possibile le proprie tracce e la direzione dell'attacco per indurre chi si difende in confusione.

Di conseguenza, anche la deterrenza – che si basa sulla volontà e capacità di rispondere e di identificare in modo inequivocabile l'avversario – è ben più difficile da praticare. Questo è il motivo per cui nel cyberspazio la difesa basata sulla deterrenza non funziona, diversamente dalla *Mutual Assured Destruction* (MAD) in ambito nucleare. Come insegna Clausewitz, una difesa efficace è sempre basata sia sulla protezione delle proprie posizioni, sia sulla capacità di condurre operazioni controffensive. Mancando il secondo elemento, nel cyberspazio ciò non è possibile, rendendo la difesa più debole rispetto all'attacco. Nonostante ad oggi siano relativamente pochi i casi verificati di attacchi informatici da parte di stati sovrani per fini politico-militari (contro l'Estonia nel 2007, la Georgia nel 2008, l'Iran nel 2009-10, la Saudi-Aramco in Arabia Saudita nel 2010, l'Ucraina nel 2014 e contro Daesh nel 2016), sono ormai numerosi i paesi che dispongono di unità specializzate in operazioni offensive di *cyberwarfare*: Stati Uniti, Cina, Russia, Regno Unito, Israele, Francia e Germania, ma anche Corea del Nord, Iran, Pakistan e India e altri. Tutti i governi, proprio come il settore privato, sono dunque costretti a investire somme sempre maggiori per la difesa e la pro-

tezione delle infrastrutture e reti informatiche, trasformando la *cybersecurity* in un vero e proprio business.

Guardando al futuro, la pervasività e diffusione di reti e computer sarà sempre maggiore (si o all'impianto di chip nel corpo umano). Tanto in ambito civile quanto in quello militare, la robotizzazione e l'intelligenza artificiale avranno un impatto crescente. Non solo molte professioni spariranno o saranno profondamente modificate, ma ci saranno sempre più armi "autonome" poiché, nonostante l'opposizione di molti, quella di una maggiore autonomia dei sistemi d'arma è, in un certo senso, una scelta obbligata: oggi, se un carro armato è pilotato da un operatore esterno, è vulnerabile a un attacco informatico che potrebbe immobilizzare il mezzo. Rendendo l'arma più autonoma, si ridurrebbero i rischi della penetrazione avversaria, con buona pace dell'etica occidentale di controllo sullo strumento militare.

Quelli qui analizzati sono comunque trend e, come tali, non rappresentano un destino predeterminato. È ancora possibile intervenire per modificarne l'andamento. Il punto di partenza è esserne informati e consapevoli.

PER SAPERNE DI PIÙ:

Giacomello, G. "Geopolitica delle Armi Autonome", *Limes* 2 -2017, pp. 253-260. Disponibile su: http://www.limesonline.com/cartaceo/geopolitica-delle-armi-autonome?prv=true.

Giacomello, G. e G. Siroli (2016) "War in Cyberspace", in: Ilari, V. (ed.) *Future Wars: Storia della Distopia Militare*, Quaderno 2016, Società Italiana di Storia Miliare, Milano: Acies Edizioni, pp. 693-701.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*, New York: Simon and Schuster.

Valeriano, B., B. Jensen e R. C. Mannes (2018), *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford: Oxford University Press, 2018.

La guerra e l'avvento dell'intelligenza artificiale.

di ***Christopher Coker***

L'intelligenza artificiale sta già trasformando le nostre vite, nel bene e nel male. Alcune imprese private la utilizzano già per gestire meglio gli indici azionari al fine di ottimizzare le loro strategie fiscali e bilanciare le azioni dei diversi portafogli: un manager (umano) professionista lo fa una volta all'anno, l'intelligenza artificiale ogni giorno. Nel 2016 una società IT di Hong Kong ha addirittura inserito un algoritmo nel suo consiglio di amministrazione.

Passando dal business alla guerra, macchine indipendenti e autonome non sono solo armi del futuro, ma sono già qui. I missili antinave a lunga gittata (*Long Range Anti-ship Missile*) semi-autonomi degli Stati Uniti possono aver bisogno di un essere umano per identificare i bersagli, ma utilizzano l'intelligenza artificiale per decidere come distruggerli. Israele usa già *Harpy*, un drone in grado di cercare e distruggere sistemi radar da solo, senza il permesso umano, vagabondando nei cieli finché non appare un bersaglio. La *Sea Hunter*, una nave anti-sottomarino statunitense, può navigare per mesi negli oceani senza nessuno a bordo alla ricerca di nemici – la versione letale del brigantino *Marie Celeste*. Se ad oggi nessun'arma completamente autonoma è stata ancora sviluppata, circa 400 sistemi d'arma semi-automatici o robotici sono attualmente in fase di sviluppo in tutto il mondo.

AlphaGo Zero, la macchina creata per giocare a Go, l'antico gioco da tavola cinese, ha chiaramente dimostrato di essere capace di imparare e sviluppare strategie creative, pianificare e risolvere i problemi grazie all'esperienza maturata. Perché ciò è importante? In guerra, così come nella vita in generale, la capacità di agire (*agency*) è sempre dipesa – almeno finora – da una serie di qualità umane: la volontà, il coraggio, la paura, l'esperienza tattica, la creatività e quello che T.E. Lawrence ha descritto come il "decimo irrazionale", garantito solamente da "istinto, affinato dal pensiero". Le macchine saranno presto in grado di fornire questo "decimo irrazionale" senza paura, stanchezza o scrupoli morali. La domanda che sorge spontanea è allora la seguente: ci sostituiranno mai?

Se le macchine svilupperanno o meno una coscienza in futuro è una questione che possiamo lasciare da parte: se succederà, sarà probabilmente fra molto tempo, anche se Ray Kurzweil, ingegnere capo di Google, ha anticipato di tre anni l'avvento della cosiddetta "singolarità tecnologica", dal 2042 al 2039. Per quanto le macchine stiano diventando, e continueranno a diventare, sempre più autonome anche quelle più complesse e sofisticate rimarranno comunque attori dipendenti ancora per qualche tempo. Mi si permetta di fornire tre spiegazioni al riguardo.

La prima e più ovvia osservazione da fare è che l'intelligenza artificiale è priva di obiettivi. Quella umana è inve-

ce una "intelligenza motivata". Grazie alla selezione naturale, siamo governati da un insieme di emozioni, istinti e pulsioni programmato per consentire di riprodurci. La selezione naturale ci dà degli obiettivi: vincere, dominare e controllare gli altri. Dobbiamo trovare l'equilibrio tra questi obiettivi e il nostro bisogno di sopravvivenza, optando per azioni a sostegno della nostra vita. Le macchine non sono motivate da alcun desiderio innato di sostenere la propria esistenza.

Dal momento che, almeno per ora, non riconosciamo intenzionalità alle macchine, riteniamo di non doverci impegnare in una relazione intelligente con loro. Il filosofo Daniel Dennett ha introdotto il termine "ordini di intenzionalità" per ragionare sul funzionamento dell'intelligenza sociale. Se credo che un'altra persona sappia qualcosa, sono in grado di gestire un ordine di intenzionalità. Se credo che questa persona creda che io sappia qualcosa, allora sono in grado di gestire due ordini di intenzionalità. Se invece credo che la stessa persona ritenga che mia moglie pensi che io sappia qualcosa, allora sono in grado di gestire tre ordini di intenzionalità. In quanto umani, incontriamo regolarmente almeno tre diversi ordini di intenzionalità nella nostra vita quotidiana. Secondo Dennett possiamo addirittura gestirne cinque. In altre parole, un'entità che non possiede motivazione è un'entità che non può vivere in società.

In seconda battuta, le macchine non solo sono prive di motivazione, ma mancano anche di aspirazioni: esse sono, per così dire, entità non-teleologiche. Cosa sto facendo su questo campo di battaglia? Perché mi sto esponendo a un tale rischio? Su cosa verte l'intero conflitto? Sono disposto a morire e, in caso affermativo, per che cosa: una religione, il mio paese, la famiglia? Tutte queste sono domande "aspirazionali" che, come tali, implicano un linguaggio teleologico che produce un senso di scopo o di fine. Trovo che questa idea sia stata espressa in modo eloquente in una lettera che il romanziere Saul Bellow scrisse a un suo amico su uno dei suoi personaggi più famosi, Augie Marsh. Augie, secondo l'autore, è l'incarnazione di un tratto umano particolare: la volontà di servire gli altri. Augie è un uomo che implora "per l'amor di Dio, fate uso di me, ma non usatemi senza scopo". Di sicuro, aggiunge Bellow nella sua lettera, il più grande desiderio umano non è tanto quello di essere usato, quanto piuttosto quello di essere utile. I giovani jihadisti, ad esempio, sono spesso disposti a cedere la propria individualità nella speranza di essere utili agli altri. Neanche le macchine più intelligenti avranno pensieri di questo tipo.

In terza battuta, come esseri umani concepiamo la nostra capacità di agire (*agency*) come determinata da un qualcosa tanto caro agli economisti: la razionalità, e non la logica. L'intelligenza artificiale è logica. E l'abbiamo creata per una ragione: costruiamo macchine che possono prendere decisioni e fare scelte esattamente nel modo in cui non possiamo farlo noi. L'idea della logica come motore delle nostre azioni ha tanti sostenitori quanti oppositori. Fra i primi, Ray Kurtzweil crede che i robot permetteranno un significativo "*human upgrade*" e guarda all'avvento dei robot autonomi come a un imperativo morale del nostro tempo. Gli oppositori, dal canto loro, insistono che ciò ridurrà il controllo dell'operatore umano, il cosiddetto *Meaningful Human Control* (MHC). La società civile ha spesso articolato i suoi ragionamenti sull'autonomia dei sistemi d'arma proprio a partire dall'importanza di un controllo "significativo" dell'operatore umano su tali sistemi. Ma quello di "controllo umano" è chiaramente un concetto contestato di per sé, mentre la perdita di tale controllo caratterizza da sempre la guerra. Lo troviamo nella vendetta, nella disumanizzazione quotidiana del nemico, nel dispiegamento di truppe inesperte o semplicemente poco addestrate, nell'emissione di ordini poco chiari da parte dei comandanti, nell'immaturità dei soldati sul campo e persino, purtroppo, nel piacere di uccidere. Ed è proprio per questa ragione che Ronald Arkin – tutt'ora alle prese con la progettazione di una coscienza che possa essere programmata nella prossima generazione di macchine – ritiene che "il semplice fatto di essere umani rappresenti il punto più debole della catena di decisioni e azioni che porta alle uccisioni (*kill chain*)" – la biologia è contro di noi per quel che riguarda il rispetto dei principi fondamentali del diritto umanitario.

Con tutta probabilità i sistemi d'arma autonomi saranno in grado di superare le prestazioni umane in *situazioni* in cui andrà applicata una moralità "limitata", cioè specifica a una certa situazione. Sono infatti proprio le situazioni in cui si trovano gli esseri umani che generalmente incoraggiano azioni immorali. L'operato delle macchine, al contrario, non dipende dalle situazioni – in gran parte perché le macchine non devono lottare con dinamiche di tipo "combatti o fuggi" come noi. Inoltre, esse non soffrono di pregiudizi – che invece predispongono gli umani a vedere il nemico in modo negativo – e non sono soggette alla tendenza umana individuata dalla psicologia sociale a rinforzare sistemi di credenza preesistenti.

Naturalmente, però, l'avvento delle macchine autonome solleva un'altra questione sulla *human agency*: noi siamo responsabili per le decisioni che prendiamo. Un essere umano ha una levatura morale esattamente per questa ragione; un robot no. In altre parole, la responsabilità di un robot sarebbe logica, non razionale, e basata sulla coerenza: si ripeterebbe sempre uguale. Ma se lo stesso criterio si applicasse agli umani, e se la logica dovesse prevalere sulla razionalità, allora assisteremmo a un cambiamento di primo ordine nella nostra stessa comprensione dell'etica. Per noi, vivere eticamente non è mai stata una questione di "ottimizzazione del bene", ma piuttosto di giusta condotta, ad esempio nei confronti dei prigionieri di guerra. Vivere eticamente implica coltivare le virtù e rifiutare di compiere azioni che non possiamo conciliare con la nostra coscienza o con il nostro senso del sé. Vivere eticamente è quindi razionale, non logico: richiede la ricerca di un equilibrio fra idee di "bene" di ordine diverso (vincere o rispettare le regole?) e la valutazione di come applicare diversi valori nelle circostanze in cui non c'è un'unica lettura di ciò che è giusto o sbagliato. E questo è probabilmente uno degli aspetti più preoccupanti dell'avvento dei *killer robots* nonostante non sia una delle argomentazioni promosse dalle campagne contro di loro. La logica può essere pericolosa perché è priva di buon senso – e il fisico Nils Bohr lo ha espresso molto bene quando ha detto a uno studente "smettila di essere così dannatamente logico e inizia a ragionare!".

In conclusione, è forse il caso di non sopravvalutare il ruolo del control-

lo umano nella guerra, e non è neanche il caso di esagerare la capacità delle macchine di sostituirlo. Dovremmo più che altro accettare il fatto che probabilmente continueremo ad avere bisogno l'uno dell'altro. Alla fine, i pericoli posti dalle macchine corrisponderanno al margine di manovra che concederemo loro per raggiungere i nostri obiettivi. E questo è rilevante, soprattutto se si sottoscrive l'affermazione di Aristotele secondo cui l'unico scopo della guerra è la pace. I droni, per esempio, hanno trasformato il modo in cui cerchiamo di controllare il cosiddetto *human terrain*, ma il successo dei loro attacchi è controverso: hanno eliminato molti dei nemici degli Stati Uniti, ma ne hanno anche creati tanti altri. Possiamo anche inventare macchine che facciano la guerra al nostro posto, ma siamo i soli in grado di fare pace tra di noi. Almeno fino al giorno in cui le macchine non si sveglieranno...

PER SAPERNE DI PIÙ:

Coker, C. (2018) "Still 'the human thing'? Technology, human agency and the future of war", *International Relations*, 32 (1), pp. 23-38. Disponibile su: http://eprints.lse.ac.uk/87629/1/Coker_Human%20Thing.pdf.

Coker, C. (2015) *Future War*. Cambridge: Polity Press.

La regolamentazione delle armi autonome: letteratura o diritto?

1. Un robot non può recar danno a un essere umano e non può permettere che, a causa di un suo mancato intervento, un essere umano riceva danno.
2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge.
3. Un robot deve proteggere la propria esistenza, purché la sua autodifesa non contrasti con la Prima o con la Seconda Legge.

di ***Andrea Spagnolo***

Quando nel 1950 Isaac Asimov elaborò le tre leggi della robotica, intorno alle quali scrisse i racconti dedicati al rapporto tra gli umani e l'intelligenza artificiale (inclusi nella celebre raccolta *Io, Robot*), mai avrebbe pensato che 70 anni dopo quelle leggi sarebbero rimaste l'unico tentativo di regolamentare l'uso delle armi autonome. È ormai divenuto realtà, infatti, l'impiego, durante i conflitti armati, di armi in grado di agire autonomamente o che, comunque, prevedono l'intervento umano solo per introdurre input molto generali o per, eventualmente, interrompere una condotta.

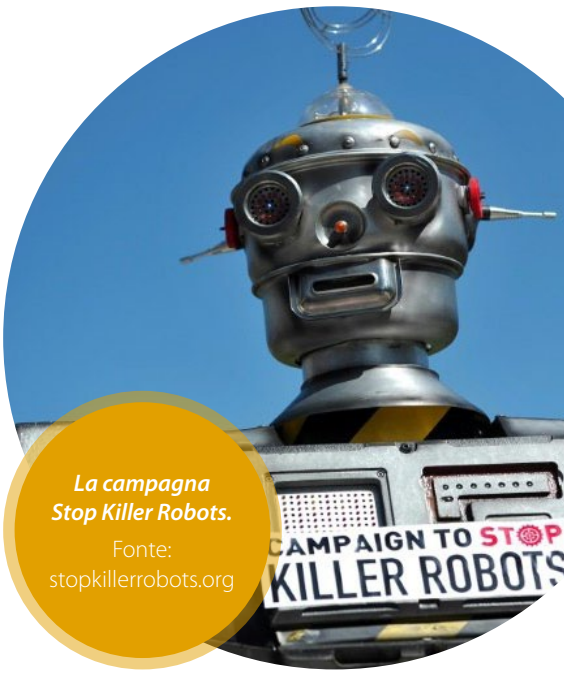
Vi è chi sostiene che le prime tracce di impiego di armi autonome durante i conflitti armati siano rappresentate dalle mine antiuomo, che una volta posizionate si attivano senza ulteriori interventi umani. Chiaramente l'autonomia di cui si discute oggi non è (solo) quella di cui godono le mine. In una prospettiva diacronica, l'esempio che aiuta a meglio comprendere il fenomeno è dato dal ricorso ai droni per operazioni di guerra o di contrasto al terrorismo internazionale. Il termine 'drone' è comunemente utilizzato per identificare velivoli pilotati da remoto che vengono utilizzati per operazioni di ricognizione e per vere e proprie 'esecuzioni mirate'. L'assenza di un pilota presente sul velivolo non rende il drone un'arma del tutto autonoma, considerato che le decisioni relative all'uso della forza, come ad esempio quella di colpire un determinato obiettivo, spetta comunque agli operatori che comandano il velivolo da remoto e che sono costantemente in grado di monitorarne le azioni.

L'impiego dei droni durante i conflitti armati rappresenta però solo una tappa del percorso di evoluzione degli armamenti. Gli stati tecnologicamente più evoluti, infatti, stanno puntando all'impiego di armi con un maggiore grado di autonomia, che siano dunque in grado di interagire senza l'intervento umano. È prova di tale tendenza la *Sea Hunter*: una nave anti-sommergibile elaborata e messa a disposizione dalla Defence Advance Research Projects Agency (DARPA) alla Marina degli Stati Uniti. Nella descrizione con cui la DARPA ha accompagnato il recente varo della *Sea Hunter*, si evince che tale nave sia dotata di caratteristiche e tecnologie idonee a rendere possibile una: "*autonomous compliance with maritime laws and conventions for safe navigation, autonomous system management for operational reliability, and autonomous interactions with an intelligent adversary*", cioè il rispetto delle leggi e delle convenzioni marittime e la gestione autonoma dell'affidabilità operativa e delle interazioni con il nemico. Tali caratteristiche sono comuni alla maggior parte delle armi autonome di cui si ha diretta conoscenza o il cui sviluppo è noto ed è utile sottolineare che la *ratio* dello sviluppo dell'intelligenza artificiale in relazione agli armamenti risiede proprio nella possibilità, per uno stato, di gestire conflitti armati senza dispiegare propri soldati, con un risparmio evidente in termini di costi umani e politici.

***Sea Hunter,* la prima nave senza equipaggio.** Fonte: DARPA.

Questo è l'argomento principale che permea le posizioni di alcuni stati nel corso delle sessioni del Gruppo di lavoro degli esperti governativi sulle armi autonome riunitosi nell'ambito della *Convention on Certain Conventional Weapons* (CCW), entrata in vigore nel 1983 con lo scopo di limitare l'utilizzo di certe armi durante i conflitti armati. La decisione di includere le armi autonome nell'agenda di un gruppo di lavoro dedicato è stata adottata dagli stati parte della CCW nel 2016, a seguito di forti pressioni da parte della società civile. Non è un caso che il primo incontro informale di esperti sulle armi autonome si sia tenuto nel 2013, anno in cui veniva lanciata la campagna *Stop Killer Robots* da parte di varie organizzazioni non governative, tra cui Human Rights Watch e Article36.

Il Gruppo di lavoro degli esperti sulle armi autonome ha finora tenuto due sessioni, l'ultima delle quali nell'aprile del 2018. Come anticipato, alcuni stati (in particolare USA e Regno Unito) sostengono che la discussione debba valorizzare i vantaggi che l'introduzione delle armi autonome porteranno nell'economia dei conflitti armati in termini di riduzione di costi umani, perché l'automazione consente un "matematico" rispetto delle norme di diritto internazionale umanitario, che diventerebbero dunque una questione di semplici – e infallibili? – variabili algoritmiche. Un secondo gruppo di stati (Brasile, su tutti) ritiene, al contrario, che le armi autonome non siano idonee a rispettare le norme fondamentali di diritto internazionale umanitario, la cui applicazione nell'ambito di un'operazione militare necessita sempre di essere giudicata e valorizzata dagli esseri umani; di conseguenza, questi stati propongono la redazione di un atto giuridico internazionale vincolante che regoli l'uso delle armi autonome nel senso di prevedere sempre la possibilità di un intervento umano. Tale posizione è altresì sostenuta dalla società civile chiamata a intervenire durante i lavori del Gruppo degli esperti; le organizzazioni partecipanti, infatti, hanno fin da subito ritenuto necessario indurre gli stati a introdurre una regolamentazione delle armi autonome fondata sul cosiddetto *Meaningful Human Control* (MHC), cioè una regolamentazione volta a proibire l'uso di armi che non prevedano in alcun modo l'intervento umano. Una posizione intermedia è sostenuta dagli stati che come Francia e Germania ritengono sufficiente che l'utilizzo delle armi autonome venga regolato dalle norme esistenti, in particolare l'Articolo 36 del Primo Protocollo aggiuntivo del 1977 alle Convenzioni di Ginevra del 1949 che obbliga gli stati parte a denunciare l'acquisizione di nuove armi, specialmente quando il loro utilizzo sia potenzialmente incompatibile con le norme che regolano l'uso della forza nei conflitti armati.



La campagna Stop Killer Robots. Fonte: stopkillerrobots.org

La polarizzazione delle tre posizioni è direttamente proporzionale agli interessi degli stati che stanno investendo (o hanno investito) maggiormente in tecnologia militare, in questo replicando le logiche dei negoziati dei trattati sui programmi nucleare. È dunque difficile prevedere oggi quale potrà essere l'esito dei lavori del Gruppo degli esperti. La posta in gioco è però molto alta. Le armi autonome, se definitivamente sganciate dall'intervento umano, consentiranno a una macchina di decidere se usare la forza letale solo sulla base di un algoritmo e dei dati che la stessa macchina sarà chiamata a raccogliere, setacciare ed elaborare. Che l'intelligenza artificiale sia in grado di rispettare i principi cardine del diritto umanitario – distinzione, proporzionalità, umanità – è tutto da dimostrare ed è particolar-

mente dubbio che una macchina sia in grado di "calcolare" la gravità dei danni collaterali di un'operazione in proporzione al vantaggio militare previsto senza che questo calcolo sia mediato e interpretato da un essere umano. Più di tutto, a lasciare perplessi è lo scenario in cui il soldato del futuro – un robot? – sia completamente sganciato da forme di responsabilità giuridica per le sue azioni. A oggi, è difficile prevedere la possibilità di processare un robot ed è altrettanto complesso ipotizzare l'applicazione del principio della responsabilità di comando, dal momento che l'intelligenza artificiale è in grado di assumere decisioni autonomamente; non è nemmeno da escludersi che il robot possa violare regole giuridiche poiché malfunzionante, ma la responsabilità del costruttore è un tema ancora più spinoso.

Il vero rischio connesso all'utilizzo delle armi autonome, dunque, è che il loro impiego conduca a una deresponsabilizzazione giuridica, prima, ed etica, poi, degli stati nella condotta delle ostilità, che rischia inevitabilmente di rendere meno costoso e, in ultima istanza, più semplice ipotizzare l'avvio di un conflitto armato. La "corsa all'arma autonoma", quindi, sebbene sia pensata per ridurre i costi (umani e politici) della guerra, rischierebbe di diventare una minaccia alla pace e alla stabilità internazionale.

Resta da sperare che le discussioni del Gruppo di lavoro degli esperti proseguano e che le posizioni si allineino nel senso di introdurre una forma di regolamentazione dell'autonomia nelle armi. È incoraggiante il *position paper* presentato dalla Cina durante la sessione di aprile 2018, dove si esortano gli stati parte della CCW a definire il grado e le modalità di coinvolgimento e intervento umano nel processo decisionale legato all'utilizzo delle armi autonome, dando per scontato che tale intervento (umano) sia necessario. È altresì incoraggiante, e interessante, notare come Google abbia deciso di non rinnovare il suo contratto con il Dipartimento di Difesa statunitense per proseguire il progetto *Maven*, nell'ambito del quale l'azienda di Mountain View forniva al Pentagono supporto tecnologico per lo sviluppo di armi in grado di decidere in completa autonomia. Se uno stato che si accinge a investire massicciamente in tecnologia (la Cina) e una delle più importanti aziende di servizi tecnologici online (Google) decidono di prendere le distanze dall'impiego di armi autonome, c'è ragione di credere che una regolamentazione internazionale sia realmente utile e necessaria.

Sullo sfondo dei lavori del Gruppo degli esperti, però, si stagliano nubi diverse e non meno preoccupanti. Il Gruppo di lavoro, infatti, ha come mandato l'utilizzo delle armi autonome durante i conflitti armati. Gli stati tecnologicamente più evoluti, tuttavia, stanno trasferendo la tecnologia militare dalla difesa agli interni, preparando la strada all'utilizzo di armi autonome per attività di polizia. Uno scenario più serio del precedente che chiama in causa ragionamenti fondati sul rispetto dei diritti umani, di cui gli stati parte della CCW non si stanno interessando. I diritti umani impongono allo stato di rendere intelligibili le proprie condotte e di provvedere a rimedi effettivi in caso di violazioni.

Al momento, non vi è traccia di una discussione sulla compatibilità delle armi autonome con i diritti umani; ciononostante, in un futuro prossimo, il poliziotto robot di Dubai che raccoglie informazioni sul traffico potrebbe non rimanere un'esperienza isolata, così come il drone semi-autonomo che sorveglia la frontiera tra le due Coree. È auspicabile che stati e società civile si concentrino anche sugli usi civili delle armi autonome ed elaborino un quadro normativo di riferimento che ne limiti l'utilizzo o, comunque, lo subordini ai diritti umani.

I tempi sono maturi perché le tre leggi della robotica non rimangano una suggestione letteraria.

PER SAPERNE DI PIÙ:

Amoroso, D. e Tamburrini, G. (2018) "The Ethical and Legal Case against Autonomy in Weapon Systems", *Global Jurist* 18, pp. 1-20. Disponibile su: https://www.degruyter.com/view/j/gj.ahead-of-print/gj-2017-0012/gj-2017-0012.xml.

Brehm, M. (2017) "Defending the Boundary. Constraints and Requirements on the Use of Autonomous Weapon Systems under International Humanitarian and Human Rights Law", *Geneva Academy of International Humanitarian Law and Human Rights*. Briefing No. 9. Disponibile su: https://www.geneva-academy.ch/joomlatools-files/docman-files/Briefing9_interactif.pdf.

Spagnolo, A. (2017) "Human rights implications of autonomous weapon systems in domestic law enforcement: sci-fi reflections on a lo-fi reality", *Questions of International Law* 43, pp. 33-58. Disponibile su: http://www.qil-qdi.org/human-rights-implications-autonomous-weapon-systems-domestic-law-enforcement-sci-fi-reflections-lo-fi-reality/.

Dal *Cybersecurity Tech Accord* a una *Digital Geneva Convention*: responsabilità, fiducia e impegno condiviso.

di ***Pier Luigi Dal Pino***

La Quarta rivoluzione industriale si presenta come un dirompente cambiamento socio-economico e una vera e propria trasformazione che interessa tutti gli aspetti della vita umana, sociale e politica. Accanto ai benefici che tale trasformazione comporta, non sono poche le criticità che necessitano di essere gestite con responsabilità e in una logica di collaborazione per poter godere dei benefici del progresso. Al contempo, però, va garantita anche la protezione dell'individuo dalle minacce che sorgono in una nuova dimensione: quella dello spazio cibernetico.

Uno sviluppo tecnologico come quello dell'intelligenza artificiale, cuore della Rivoluzione odierna, impone ad esempio una riflessione importante che deve necessariamente mettere l'uomo al centro del progresso tecnologico, difenderne i diritti fondamentali – come la non discriminazione e la privacy – e salvaguardarne la dignità e l'inclusione sociale. In quest'ottica non è possibile prescindere da una riflessione sulla dimensione della sicurezza, concepita come ulteriore diritto fondamentale degli individui. Infatti, se da un lato stiamo assistendo a una corsa agli armamenti informatici da parte di nazioni che investono sempre più nello sviluppo di armi e tecnologie destinate a scopi militari e civili (le cosiddette tecnologie *dual use)*, dall'altro ci stiamo rendendo conto dell'entità dei danni che armi "invisibili", come quelle cibernetiche, possono infliggere ai cittadini. Nel maggio 2017, ad esempio, l'attacco di *ransomware* "WannaCry" ha colpito più di 200.000 computer in più di 150 paesi, non solo danneggiando gli apparati informatici ma causando anche pesanti ripercussioni su servizi e persone. L'attacco – attribuito per la prima volta a uno stato, la Corea del Nord – ha costituito un importante campanello di allarme a livello internazionale e ha messo in luce debolezze e vulnerabilità rilevanti tanto per la sicurezza nazionale quanto per quella umana. Non da ultimo, infatti, si assiste oggi a un aumento degli attacchi intenzionalmente diretti ai civili, anche da parte degli stati.

Brad Smith durante i lavori delle Nazioni Unite a Ginevra, novembre 2017.
Fonte: Elma Oki/ UN Photo.

A fronte di tutto ciò, Microsoft Corporation si è fatta portavoce dell'esigenza di una Convenzione digitale di Ginevra (*Digital Geneva Convention*), cioè di una proposta che conduca a un insieme di norme e accordi internazionali volti a proteggere e difendere i civili dagli attacchi cibernetici. Come ricordato da Brad Smith, presidente di Microsoft, durante un evento organizzato dalle Nazioni Unite a Ginevra il 10 novembre 2017, la *cybersecurity* è diventata chiaramente una delle questioni più importanti del nostro tempo. La stabilità del cyberspazio e la tutela degli individui sono infatti due elementi cruciali che vanno considerati e gestiti a partire da due principi cardine: (*a*) la responsabilità, ovvero la tutela dei civili come fine imprescindibile dell'uso delle tecnologie e la consapevolezza della risonanza delle proprie azioni, e (*b*) la fiducia, da infondere sia nel rapporto con individui e clienti sia tra gli attori coinvolti nella definizione e nella risoluzione delle sfide nel cyberspazio.

L'industria digitale non solo riveste un ruolo preponderante in termini di capacità e di competenze in ambito di *cybersecurity*, ma è solitamente in prima linea nella reazione e gestione di attacchi informatici. Sulla base di questo senso di responsabilità condivisa e con il fine di apportare il proprio contributo alla stabilità del cyberspazio più di 40 aziende tecnologiche, tra cui Microsoft, hanno firmato lo scorso aprile e nei mesi successivi il *Cybersecurity Tech Accord*, un impegno pubblico fondato su quattro principi:

- La protezione dei propri utenti e clienti ovunque essi si trovino – siano essi individui, organizzazioni o governi – e indipendentemente dalle loro conoscenze tecniche, dalla loro cultura oppure dalle motivazioni dell'aggressore, siano queste a scopo criminale o di matrice geopolitica. Le aziende firmatarie si impegneranno a progettare, sviluppare e fornire prodotti e servizi che privilegino la sicurezza, la privacy, l'integrità e l'affidabilità, riducendo così la probabilità, la frequenza e la gravità delle vulnerabilità. Ciò include una maggiore protezione delle istituzioni e dei processi democratici in tutto il mondo.
- Il contrasto agli attacchi informatici contro cittadini innocenti e imprese, impegnandosi a proteggere i prodotti e i servizi tec-

nologici dalla manomissione e dallo sfruttamento durante le fasi di sviluppo, progettazione, distribuzione e uso. Le aziende si sono altresì impegnate a non aiutare i governi a lanciare attacchi informatici contro cittadini e imprese.

- Il rafforzamento di capacità cibernetiche che permettano agli utenti, ai clienti e agli sviluppatori di incrementare la protezione della *cybersecurity* attraverso una maggiore condivisione di informazioni e strumenti che consentano loro di comprendere le minacce attuali, prevedere quelle future e proteggersi da esse. Inoltre, i firmatari sosterranno la società civile, i governi e le organizzazioni internazionali nei loro sforzi per far aumentare la sicurezza nel cyberspazio e per sviluppare ulteriori capacità in questo senso, tanto nelle economie sviluppate quanto in quelle emergenti.
- La collaborazione fra aziende e gruppi che condividono la stessa visione per migliorare la sicurezza informatica. Questo include partnership formali e informali con l'industria, la società civile e l'accademia, attraverso tecnologie proprietarie e *open-source* al fine di migliorare la collaborazione tecnica, la divulgazione coordinata delle vulnerabilità e la condivisione delle minacce, nonché per ridurre al minimo i rischi e i possibili danni nel cyberspazio. Inoltre, si incoraggeranno la condivisione di informazioni a livello globale e gli sforzi di attori civili per identificare, prevenire, rilevare e rispondere agli attacchi informatici, recuperare dai danni causati e garantire risposte flessibili per la sicurezza del più ampio ecosistema tecnologico globale.

L'importanza del *Cybersecurity Tech Accord* è duplice: da un lato, esso costituisce un *unicum* nel campo tecnologico e nella gestione del cyberspazio, segno di un impegno condiviso e della necessità di dare sostanza ai principi di responsabilità e fiducia nelle tecnologie. Dall'altro, la sua visione è accompagnata da azioni concrete che le aziende implementeranno, fornendo pertanto un contributo pragmatico all'esigenza di un cyberspazio stabile e sicuro.

Sebbene nessun accordo internazionale sia mai perfetto, il mondo ha già tratto benefici e visto importanti miglioramenti grazie alla stipula di convenzioni globali in materia di armamenti, come dimostrato dal Trattato sulla non-proliferazione delle armi nucleari o dalla Convenzione sulle armi chimiche. Accanto all'impegno dell'industria, è quindi importante che, anche nell'ambito della *cybersecurity*, iniziative concrete pervengano dai governi: la ratifica di una Convenzione digitale di Ginevra, ad esempio, creerebbe un quadro giuridicamente vincolante per governare il comportamento degli stati nel cyberspazio. Nonostante la formulazione e l'attuazione di norme giuridicamente vincolanti richiedano tempo, le conseguenze di un'eventuale inazione sono oggi inaccettabili. La complessità e la vastità della tematica non possono quindi rappresentare una giustificazione per il mancato impegno degli stati al raggiungimento di obiettivi concreti di stabilità e sicurezza nel cyberspazio.

Sebbene ci sia urgenza nel rispondere alle crescenti aspettative in questo senso, è possibile procedere in modo incrementale con misure intermedie al fine di conseguire accordi realmente condivisi che man mano si estendano a tutti gli aspetti che la gestione del cyberspazio richiede. Come per la non-proliferazione nucleare, gli stati dovrebbero avanzare con un approccio *non-offensive* nello spazio cibernetico, al fine di ridurre il rischio di attacchi e conflitti. In tempo di pace, alcune regole che raggiungerebbero questo fine potrebbero essere le seguenti:

- Astenersi dall'inserimento di *backdoor* (cioè "porte di servizio" che permettono di aggirare le difese di un sistema informatico e dunque accedervi) nei prodotti della tecnologia commerciale di massa;
- Accettare una politica chiara per acquisire, conservare, proteggere, utilizzare e segnalare vulnerabilità e debolezze;
- Limitare lo sviluppo di armi informatiche, garantendo il loro controllo in un ambiente sicuro;
- Acconsentire a limitare la proliferazione delle armi informatiche;
- Limitare l'impegno in operazioni offensive e dedicarsi esclusivamente ad attività difensive per evitare danni di massa ai civili;
- Assistere gli sforzi del settore privato per individuare, contenere e rispondere ad attacchi informatici.

Un altro aspetto fondamentale per la stabilità e la sicurezza del cyberspazio è la necessità di creare una *Cyberattack Attribution Organization*, ovvero un'organizzazione internazionale di attribuzione di responsabilità, volta a rafforzare la fiducia degli utenti nei confronti del mondo digitale. Se nel mondo "reale" quando qualcuno ruba o danneggia la proprietà fisica, infatti, gli investigatori possono raccogliere prove da presentare in tribunale; nel mondo "digitale" questo è molto più complicato, soprattutto se consideriamo il numero limitato di esperti capaci di reperire prove inequivocabili di un avvenuto attacco informatico. Se poi tale attacco è sponsorizzato da uno stato, dimostrarne la responsabilità diventa una sfida ancora più complessa. Ad oggi non esiste un'organizzazione o una struttura indipendente che possa presentare un'analisi politicamente neutrale basata su fatti verificati. L'incremento quantitativo e qualitativo delle sfide alla *cybersecurity* hanno però fatto emergere il bisogno di un organismo di attribuzione che riceva e valuti le prove relative a un sospetto *cyberattack* e che possa essere in grado di individuarne i responsabili. Un'organizzazione simile dovrebbe sfruttare la collaborazione fra settore pubblico e privato e avvalersi di esperti in *cyberforensics* o discipline correlate, provenienti dal mondo aziendale e in grado di analizzare le tecnologie e le tecniche alla base di un attacco. Un simile lavoro di ricerca e analisi potrebbe essere altresì supportato dagli strumenti resi disponibili dalla tecnologia cloud, assicurando così che le prove relative a particolari attacchi siano raccolte e presentate in modo tale da essere comprese dal pubblico e utilizzate dagli esperti governativi.

Il *Cybersecurity Tech Accord*, siglato dalle principali imprese informatiche che offrono servizi e soluzioni digitali, dimostra l'impegno del settore privato a elaborare un insieme comune di principi e comportamenti per proteggere i civili nello spazio cibernetico. Ciò non

Le iniziative di Microsoft.

Fonte: www.irinnews.org

significa solamente accordarsi su azioni che l'industria dovrebbe intraprendere o meno, ma anche condividere obiettivi, risorse ed energie per migliorare la *cybersecurity* a livello globale. Mentre le aziende tecnologiche hanno una responsabilità primaria e si trovano, a tutti gli effetti, in prima linea nell'affrontare queste problematiche, sarebbe un errore pensare che il settore privato sia in grado da solo di impedire o arrestare il rischio di attacchi informatici. Una tematica così complessa non può che richiedere uno sforzo e un approccio di collaborazione multidisciplinare tra le diverse compagini sociali, includendo il settore pubblico, le aziende private, il mondo accademico, le organizzazioni civili e quelle non governative. È fondamentale che gli stati reagiscano al campanello d'allarme lanciato da "WannaCry" e dai tanti attacchi informatici che, quasi quotidianamente, accendono i riflettori sulla necessità impellente di adottare un sistema di regole e norme che protegga i civili nello spazio cibernetico, anche in tempo di pace. Chiunque interagisca con o dipenda dal cyberspazio deve essere messo nelle condizioni di aver fiducia nella tecnologia che utilizza. Il mondo ha bisogno di una *Digital Geneva Convention*, così come di altre iniziative analoghe e complementari.

PER SAPERNE DI PIÙ:

Charney S. et al. (2016) *From Articulation to Implementation: Enabling progress on cybersecurity norms*. Microsoft Corporation. Disponibile su: https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms.

Cybersecurity Tech Accord. Disponibile su: https://cybertechaccord.org/.

Microsoft Corporation (2017) "A Digital Geneva Convention to protect cyberspace", *Microsoft Policy Papers*. Disponibile su: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

Microsoft Corporation (2017) "An attribution organization to strengthen trust online", *Microsoft Policy Papers*. Disponibile su: https://www.microsoft.com/en-us/cybersecurity/content-hub/an-attribution-organization-to-strengthen-trust-online.

Smith, B. (2017) "The need for a Digital Geneva Convention", *The Official Microsoft Blog*. Disponibile su: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

La comunicazione digitale degli attivisti come lente di analisi del conflitto siriano.

di ***Gioachino Panzieri***

La rappresentazione di un conflitto finisce molto spesso per diventare un fattore di influenza del conflitto stesso; per questa ragione, i media e il controllo della produzione mediatica costituiscono degli strumenti tenuti accuratamente in considerazione dagli analisti. Nel contesto mediatico internazionale costruitosi attorno al conflitto siriano, è possibile scorgere l'evoluzione di una specifica pratica di comunicazione che ha avuto un ruolo determinante nella logistica della rivoluzione sin dal 2011. Si tratta dell'attivismo digitale, circoscritto inizialmente alla dimensione locale e in seguito trasformato in un nuovo processo di informazione che permette di fare luce sul punto di vista dei cittadini e delle comunità in Siria durante la guerra.

In una prospettiva di *human security*, l'era digitale della comunicazione globalizzata ha prodotto mutamenti paradigmatici nei rapporti tra i media e il potere: la popolazione locale non rappresenta più unicamente l'oggetto dell'informazione prodotta dall'esterno, ma, al contrario, può ora essere riconosciuta come soggetto, attore, agente di informazione diffondibile a livello internazionale. Lo stesso può dirsi della *digital community* a cui l'informazione si rivolge: non più mera destinataria, ma potenziale vettore di trasmissione. Nel caso siriano, la produzione mediatica online si è rivelata fin dall'inizio della rivoluzione una specola per osservare la partecipazione dei cittadini siriani nel conflitto, così come nella narrazione dello stesso.

Tuttavia, la maggior parte dell'informazione diffusa dai media *mainstream* in Europa ha seguito almeno due principali linee guida: la prima dà priorità alle operazioni militari e alle analisi geopolitiche o economiche, in cui le condizioni e le istanze sociopolitiche dei cittadini sono risolutamente escluse dai termini quantitativi della rappresentazione; la seconda ha legittimato logiche mediatiche di spettacolarizzazione e vittimizzazione profondamente nocive per la reale *agency* politica dei siriani. In quest'ultimo caso, i cittadini, sebbene al centro dell'immagine prodotta, costituiscono l'oggetto privo di voce delle violenze perpetrate e non il soggetto dell'informazione, assecondando un apparato discorsivo che predilige un punto di osservazione esterno e conduce inevitabilmente verso la disumanizzazione.

L'attivismo digitale per la causa siriana diretto all'opinione pubblica internazionale può essere osservato come uno strumento in grado di contrapporsi a entrambe le dinamiche appena descritte, tentando di portare al centro della comunicazione la società civile siriana, la complessità della sua condizione e delle simultanee posizioni che ha assunto nel corso del conflitto. Uno degli obiettivi principali di questa azione è infatti quello di dare priorità alla pace intesa come un processo politico che abbia al suo nucleo gli interessi dei cittadini.

Oltre a essere praticato dai siriani stessi, l'attivismo digitale per sua stessa natura veicola un'informazione che si concentra sulla dimensione più "umana" – non umanitarista – del conflitto, ovvero sulle necessità socio-economiche dei cittadini, le loro rivendicazioni politiche, le esperienze di resistenza alla guerra e di costruzione della pace vissute e testimoniate dai siriani negli ultimi anni, nonché sull'evoluzione di tali esigenze ed esperienze.

Il processo dinamico messo in atto consente di far cadere i muri del panorama mediatico, offrendo uno stimolo di studio non indifferente per il superamento delle frontiere della *conflict analysis* in merito ai processi di comunicazione e di partecipazione. Promuovendo una comprensione non statica ma rispettosa della fluidità che caratterizza la sfera sociale del conflitto, alcuni attivisti digitali sembrano presentarsi in qualità di mediatori – non esterni, bensì interni – tra la comunità siriana e la comunità globale, in quanto vicini alle strutture sociali, politiche e culturali dentro cui il conflitto siriano si inserisce, rivelandosi in grado di tradurle per un pubblico internazionale.

In particolare, sul web è possibile rintracciare la presenza di un articolato *network* di realtà digitali di informazione principalmente autoctone, ma spesso disseminate fuori dal territorio nazionale in seguito all'*escalation* del conflitto o per altre ragioni di migrazione. Tali realtà si dedicano costantemente alla causa siriana attraverso modalità differenti: riportando le testimonianze dirette delle persone coinvolte e colpite dal conflitto; documentando dettagliatamente le violazioni dei diritti umani e civili sul campo (*Violations Documentation Centre*); pubblicando appelli per un processo di pace inclusivo e partecipato o diffondendo comunicati per posizionarsi in merito a determinati accadimenti (si vedano gli *statements* del

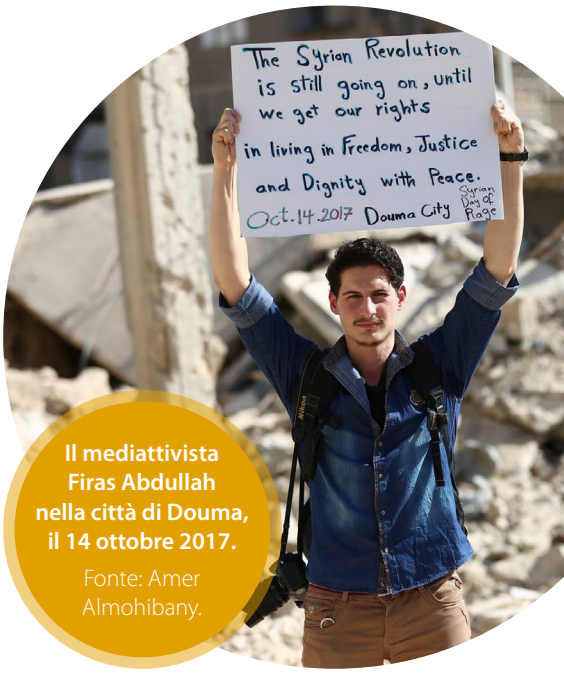
Syrian Centre for Media and Freedom of Expression); o ancora, denunciando le scelte della comunità internazionale o di altri attori – anche informali e locali – rilevanti nel conflitto; facendo luce sui numerosi processi di democratizzazione dal basso, sui casi di auto-organizzazione locale, di opposizione pacifica alla guerra, sugli episodi di lotta agli estremismi e altre iniziative di costruzione di alternative alle istituzioni preesistenti; infine, non mancando di avanzare proposte dirette a governi e istituzioni internazionali (ad esempio nei *reports* di *The Syria Campaign*).

Manifestazione nella città di Daraya nel marzo 2016.
Fonte: enabbaladi.org

Grazie all'operazione di produzione, traduzione e diffusione di questi contenuti (in Italia è di rilievo il lavoro del blog *Le Voci della Libertà*), è possibile elaborare una riflessione sul processo di *advocacy* avviato dagli attori in questione, inteso come reazione civile finalizzata a influenzare l'evoluzione del conflitto – o meglio, il processo di *peacebuilding* – attraverso azioni di informazione e comunicazione, sensibilizzazione, mobilitazione e *lobbying*.

Un riconoscimento dovuto ad alcune organizzazioni di attivisti digitali è quello di veicolare un'informazione qualitativa che tenga in vita la connessione tra gli accadimenti del conflitto e la storia del popolo che lo vive. Non di rado, l'informazione più immediatamente accessibile sul conflitto tende a focalizzarsi sull'attualità degli eventi, dimenticando o trascurando la rivoluzione e le cause profonde che hanno portato il popolo siriano a sollevarsi nel 2011 sulla spinta di una richiesta di libertà civile e politica, giustizia sociale, emancipazione economica e autodeterminazione, in opposizione a un regime autoritario rimasto al potere per i quarant'anni precedenti, che ha represso ogni forma di pluralismo e soffocato ogni germe di contestazione. Queste istanze, evolute e profondamente trasformate nel corso del conflitto, rappresentano il primo oggetto dell'informazione elaborata da una parte degli attivisti siriani che si muovono sul web per estendere il raggio dell'azione di *advocacy* di cui si fanno promotori (si osservi ad esempio l'operato dei giornalisti Fouad Roueiha e Rami Jarrah sui *social network*). Tale informazione agisce in corrispondenza di un'attenzione nei confronti della dimensione temporale di lungo periodo, "riattivando" una memoria storica essenziale per il processo di trasformazione del conflitto. Secondo questo approccio di analisi, infatti, le emergenze concrete che si verificano nel presente sono da considerare necessariamente come un'espressione del più ampio sistema di trame storiche e relazionali da cui il conflitto ha origine. I tempi dei processi socio-politici vissuti dalle società trascendono i tempi delle offensive militari e delle azioni governative, ed è pertanto necessario ricercare delle lenti allargate sul passato e sul futuro per facilitare una reale comprensione delle esigenze e delle capacità locali, così come per permettere la conseguente elaborazione di una visione legittima per il futuro. Partire dallo sguardo e dalla voce dei cittadini siriani per condurre tali analisi può considerarsi un esercizio quantomeno appropriato; in questo senso, lo strumento di comunicazione digitale sembra prestarsi allo scopo.

È certo, tuttavia, che nel mare magnum dell'informazione presente sulle piattaforme digitali e sui social *media* tale strumento viene largamente utilizzato anche da attori che non hanno alcun interesse nella pace sostenibile in Siria e che, al contrario, perseguono finalità di guerra e di repressione, diffondono ideologie estremiste o promuovono discorsi d'odio. Non sarebbe dunque prudente "romanticizzare" il canale digitale di per sé. La forma democratica della comunicazione digitale mostra infatti anche i suoi effetti perniciosi. A tal proposito, i casi di strumentalizzazione politica e manipolazione delle tecnologie di comunicazione sono ben noti anche al di fuori dei contesti di guerra. L'impiego ricreativo dei *social network*, inoltre, potrebbe apparentemente ostacolare la possibilità di visualizzarli come strumenti adatti a ricercare un punto di vista approfondito e critico. Infine, l'articolazione orizzontale e la frammentazione di questi nodi di informazione rende gli effetti di tale forma di comunicazione poco misurabili, impedendo un'operatività automatica in termini di *policies*. Sono infatti molti i fronti toccati dalle organizzazioni e dagli attori in questione (si pensi ai progetti compiuti da *Rethink Rebuild Society*): gli obiettivi specifici del loro lavoro possono divergere, così come i contesti in cui sono insediati e gli attori con i



Il mediattivista Firas Abdullah nella città di Douma, il 14 ottobre 2017.
Fonte: Amer Almohibany.

quali tentano di dialogare e collaborare. Ciononostante, è possibile individuare nel loro procedere una struttura comune che suggerisce uno schema teoricamente ibrido, promuovendo l'emancipazione locale nel processo di pace senza respingere il sostegno internazionale, che è stato anzi al centro della richiesta di solidarietà espressa da molti cittadini siriani.

Per quanto risulti quindi difficoltoso riconoscere un'efficacia concreta e un'influenza istantanea sul conflitto al lavoro di quegli attivisti che tentano di diffondere le ragioni e le istanze sociali in rete, è possibile individuarvi la rilevanza di un processo partecipativo di informazione al servizio della storia che potrebbe avere come effetto un'influenza di più ampio respiro all'interno di un progetto educativo di lungo termine.

Il modello di comunicazione qui ridotto per comodità al termine di "attivismo digitale" sembra rivelarsi uno strumento in parte capace di catturare la complessità propria del conflitto a partire dal basso – anche in ragione della sua maggiore libertà dai rapporti di potere instaurati da e tra i media – restituendo un'informazione paradossalmente più accessibile ai cittadini, investiti da un processo che esprime un forte potenziale di politicizzazione sia per i produttori che per i fruitori dell'informazione.

PER SAPERNE DI PIÙ:

Ivie R. (2005) "Web-Watching for Peace-Building in the New Communication Order", *Javnost – The Public*, 12:3, pp. 61-77. Disponibile su: https://www.dlib.si/stream/URN:NBN:SI:DOC-C014EOXK/2e9f7c39-6e58-4258-a377-0d66e55c1d4c/PDF.

Trombetta, L. (2017) "Syria – Media Landscape", *European Journalism Centre (EJC)*. Disponibile su: https://medialandscapes.org/country/pdf/syria.

Tellidis I. e Kappler, S. (2016) "Information and Communication technologies in peacebuilding: Implications, opportunities and challenges", *Cooperation and Conflict*, Sage Publications, Vol. 5, No. 1, pp. 75-93. Disponbile su: https://doi.org/10.1177/0010836715603752.

Declich, L. e Pinto, C. (2017) (a cura di) *Prima che parli il fucile. Omar Aziz e la rivoluzione siriana*. Messina, Mesogea. Anteprima disponibile su: http://www.mesogea.it/images/anteprime/primacheparli(estratto).pdf.