Cyberwar: come cambia la guerra in uno spazio tutt'altro che virtuale

Stefano Pietropaoli

Sin dal tempo in cui ci si affrontava con pugnali di selce e lance di faggio, le guerre sono state inesorabilmente legate alle tecnologie che i contendenti avevano a disposizione.

Non deve dunque stupire che, allo stesso modo della fusione del bronzo, della produzione della polvere da sparo o della fusione dell'atomo, anche lo sviluppo dell'informatica abbia comportato una radicale trasformazione del modo di fare la guerra.

Questo mutamento è ben più profondo di quanto si possa cogliere a un primo sguardo. Lo spazio cibernetico è diventato uno dei campi di battaglia su cui si misurano le piccole e le grandi potenze. Dopo la guerra terrestre, quella marina, quella aerea e quella sottomarina, è arrivato dunque il tempo di una guerra combattuta in una nuova dimensione spaziale. Ma sarebbe errato immaginare questa cyberwar come una guerra "virtuale".

L'idea di "guerra cibernetica" potrebbe forse sollecitare l'immagine di un teatro di guerra immacolato, calcato da tecnici in camice bianco e in cui l'unico suono udibile è il rapido ticchettio delle dita sulla tastiera di un calcolatore.

Il primo problema della cyberwar sta proprio nella rappresentazione illusoria di una guerra meno violenta e brutale rispetto allo scontro tra falangi oplitiche, cavallerie medievali o artiglierie ottocentesche. Come ogni guerra, anche la guerra cibernetica ha lo scopo di colpire obiettivi ritenuti fondamentali per assicurarsi la vittoria sul nemico. E, come in ogni guerra, anche nella guerra cibernetica il migliore equipaggiamento delle truppe può risultare un vantaggio tattico decisivo.

Le tecnologie informatiche sono ormai impiegate stabilmente nei conflitti armati. Del resto, l'informatica era stata decisiva già durante il secondo conflitto mondiale, quando la potenza computazionale dei primi elaboratori venne impiegata per decifrare i messaggi in codice dell'esercito tedesco. E non dimentichiamo che internet è stato sviluppato inizialmente per finalità militari durante la Guerra fredda, in uno scenario in cui era fondamentale elaborare strategie di comunicazione alternative in caso di conflitto termonucleare.

L'uso delle tecnologie informatiche oggi riguarda il miglioramento dei sistemi di puntamento di un missile, la possibilità di crittografare comunicazioni strategiche con sistemi inimmaginabili fino a pochi anni fa, o la capacità di colpire un bersaglio distante migliaia di chilometri grazie a un drone comandato via satellite. In altre parole, le tecnologie informatiche hanno senz'altro innovato profondamente gli strumenti "classici" della guerra (armi, mezzi, comunicazioni, etc.). Ma non si tratta soltanto di questo.

Le tecnologie informatiche costituiscono oggi nello stesso tempo uno

strumento e un obiettivo della guerra. È in quest'ultimo senso che la guerra contemporanea in alcuni casi diventa una guerra talmente diversa dalle forme precedenti da meritarsi l'appellativo di cyberwar.

Le armi impiegate sono diverse da quelle cui siamo abituati, ma non per questo sono meno distruttive. Le infrastrutture informatiche di ogni paese sono ormai essenziali tanto per il funzionamento dell'apparato statale quanto per l'erogazione di servizi a favore della popolazione.

In quanto tali, sono obiettivi privilegiati di un attacco cibernetico. Si badi bene: non si tratta soltanto di rendere irraggiungibile un determinato sito (solitamente tramite attacchi DDoS), o di violare database riservati per poi rivelarne il contenuto. Un attacco cibernetico può produrre danni materiali e perdite umane in maniera del tutto sovrapponibile a un'arma analogica.

Con un malware è possibile bloccare l'approvvigionamento di energia elettrica, gas o petrolio di un paese (basti ricordare l'episodio della Colonial Pipeline del maggio 2021, che ha bloccato l'impianto che eroga il 45% delle forniture di carburante per la costa est degli USA), aprire a distanza le chiuse di una diga, mandare in tilt la gestione del traffico stradale, aereo o ferroviario (con gli esiti che si possono immaginare), oppure danneggiare un impianto nucleare.

A quest'ultimo proposito, basti ricordare che nel 2010 la centrale iraniana di Natanz è stata colpita da un attacco cibernetico che ha provocato la distruzione della sezione adibita all'arricchimento dell'uranio. Attraverso un malware denominato Stuxnet, sono stati inviati comandi anomali a più di mille centrifughe, che hanno subito in questo modo un'accelerazione talmente alta da comportarne la rottura. Contemporaneamente, Stuxnet ha consentito di alterare i dati di controllo del sistema, impedendo che il problema venisse avvertito in tempo utile per mettere in sicurezza l'impianto. In questo modo l'attacco è stato scoperto quando il processo era ormai irreversibile.

Il conflitto in corso tra Russia e Ucraina è soltanto l'ennesima, eclatante conferma di questo nuovo modo di fare la guerra (che si affianca alle sue manifestazioni analogiche), i cui prodromi potevano essere ravvisati già dalla fine del secolo scorso e che si è rivelato per la prima volta in maniera chiarissima nel 2007, quando l'Estonia è stata protagonista di quella che viene ricordata come Web War One.

Per almeno tre settimane i sistemi informatici delle massime istituzioni politiche, degli istituti finanziari e dei mezzi di comunicazione del paese baltico sono stati oggetto di un massiccio attacco informatico (di cui, ovviamente, il primo sospettato è stata la Russia) che ne ha impedito il regolare funzionamento.

L'anno successivo la Nato ha voluto inviare un segnale dal chiaro valore simbolico istituendo nella capitale estone il suo quartier generale per la difesa delle infrastrutture strategiche occidentali: il Cooperative Cyber Defence Centre

of Excellence (CCDCOE). Nell'ambito delle attività di questo gruppo di esperti è stata promossa la redazione di un documento che inquadrasse il problema dell'applicabilità del diritto internazionale alle operazioni di cyberwar. Il gruppo di esperti incaricato della ricerca ha elaborato alcune regole applicabili alla guerra cibernetica nel "Tallinn Manual on the International Law Applicable to Cyber Warfare" del 2013, aggiornato e ampliato nel febbraio 2017.

Uno dei punti centrali del Manuale è la questione se alla cyberwar sia applicabile o meno il diritto internazionale dei conflitti armati. In altre parole: un attacco cibernetico può essere considerato "minaccia o uso della forza" contro l'integrità territoriale o l'indipendenza politica di uno Stato, alla stregua di un attacco "analogico"?

Se la risposta è affermativa, le conseguenze sul piano giuridico (oltre che politico) di un attacco cibernetico sono di estrema importanza. Tra queste, una delle più rilevanti è il riconoscimento allo Stato aggredito del diritto di reagire con la forza quando l'attacco cibernetico raggiunge il livello di conflitto armato. Si configura, cioè, un'ipotesi di legittima difesa che sostanzialmente consente allo Stato attaccato ciberneticamente di usare la forza.

Il Manuale di Tallinn risulta assolutamente coerente con gli obiettivi fissati dalla Cyber Strategy elaborata dal Dipartimento della Difesa statunitense negli ultimi anni, mentre non prende minimamente in considerazione le diverse interpretazioni e sensibilità di attori internazionali fondamentali come Cina e Russia. Nato e Stati Uniti infatti sostengono unanimemente non soltanto che il diritto internazionale si applichi al cyberspace, ma anche che la difesa di quest'ultimo sia inclusa tra i doveri di difesa collettiva per i quali è stata istituita l'Alleanza.

Lo scopo generale della difesa dello spazio cibernetico è quello di prevenire o almeno contenere i danni a infrastrutture critiche, sia militari sia civili. Ma quest'obiettivo deve essere raggiunto in uno scenario in cui sono saltate le distinzioni del vecchio diritto internazionale, come quelle tra civile e militare, neutrale e belligerante, prigioniero e combattente: la cyberwar non soltanto non viene dichiarata — e quindi ogni attacco è un attacco a sorpresa — ma, soprattutto, non rende riconoscibile chi sta attaccando, perché, quando e come sta conducendo l'attacco, quali saranno le prossime mosse, come si dovrebbe reagire, e così via.

Dietro la maggioranza degli attacchi cibernetici ci sono ancora gli Stati nazionali, ma numerosi sono i casi di operazioni ricollegabili a entità non statuali (basti pensare alle attività di gruppi come Anonymous). In questo senso si parla ormai da alcuni anni di "cyberterrorismo" ad indicare gli attacchi perpetrati da gruppi di *hacktivist* che sfruttano le tecnologie informatiche al fine di generare paura o intimidire una società ritenuta nemica sulla base di un giudizio ispirato a una precisa ideologia.

Anche in questa prospettiva, il conflitto in corso testimonia che entità quali il

collettivo bielorusso Conti o l'organizzazione russa nota come Killnet sono in grado di sferrare attacchi capaci di mettere in crisi le infrastrutture strategiche di paesi considerati nemici (Italia compresa).

Occorre prendere molto sul serio queste minacce. Nessuno, oggi, può considerarsi immune alla guerra cibernetica.

Suggerimenti di lettura:

Bauzon S., *Cyberterrorismo/Cyberwar*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Giappichelli, Torino, 2024, pp. 120-122.

Campagnoli M.N., *I nuovi volti del terrore: dal terrorismo islamico al cyber terrorismo*, Key, Milano, 2017.

Iaselli M., Caria G.B., *Cybersecurity e cyberwarfare. Diritto, tecnologia e sicurezza*, Roma, EPC Editore, 2022.

Pietropaoli S., *Guerra cibernetica*, in Id., *Informatica criminale. Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2*, Giappichelli, Torino, 2025, pp. 53-71.

Pozzi P., Bozzetti M. (a cura di), *Cyberwar o sicurezza? II Osservatorio criminalità ICT*, Milano, FrancoAngeli, 2001.

Auto a guida autonoma: l'IA alla prova dell'etica

Piero Sansò

Lo sviluppo di veicoli capaci di navigare e operare autonomamente prospetta di trasformare radicalmente il settore dei trasporti, le forme dell'urbanistica e la quotidianità di un enorme numero di individui.

Fra i benefici promessi rientrano l'aumento della sicurezza stradale (l'errore umano resta di gran lunga la causa più alta di mortalità su strada), l'accesso alla mobilità da parte di categorie prima escluse o fortemente svantaggiate e l'efficienza del traffico e della logistica.

La tabella di marcia per l'introduzione di questa tecnologia, rispetto alle dichiarazioni fin troppo ottimistiche di qualche anno fa, è stata posticipata.

Con l'aumento del livello di automazione, emergono sfide sempre più complesse e rilevanti, non solo dal punto di vista tecnologico, ma anche etico e normativo.

I sei livelli di automazione della guida autonoma, come è noto, sono definiti dalla Society of Automotive Engineers (SAE) e vanno da 0 a 5.

Ciascun livello indica il grado di autonomia del veicolo, ovvero quanto il sistema di guida assistita o autonoma può gestire il veicolo senza l'intervento umano.

Livello 0 – Nessuna automazione: il conducente ha il controllo completo del veicolo in ogni momento, con sistemi di assistenza che possono fornire solo avvisi o assistenza.

Livello 1 – Assistenza alla guida: alcune funzioni sono automatizzate per assistere il conducente in attività specifiche, come il controllo della velocità tramite il cruise control adattivo o l'assistenza alla sterzata, ma non entrambi contemporaneamente. Il conducente deve sempre mantenere il controllo.

Livello 2 – Automazione parziale: il veicolo può gestire simultaneamente sia lo sterzo che la velocità. Tuttavia, il conducente deve essere sempre vigile e pronto a riprendere il controllo immediatamente.

Livello 3 – Automazione condizionata: il veicolo può gestire tutte le funzioni di guida in condizioni specifiche, come su strade ad alta velocità, senza l'intervento continuo del conducente. Il conducente deve comunque essere pronto a intervenire se il sistema lo richiede.

Livello 4 – Alta automazione: il veicolo può guidare autonomamente senza l'intervento del conducente in determinate condizioni operative. Fuori da queste condizioni, il veicolo richiede assistenza umana.

Livello 5 – Automazione completa: il veicolo è completamente autonomo in ogni contesto e non richiede il conducente. Non ci sono limitazioni operative e il veicolo non necessita di volante o pedali.

Ad oggi la maggior parte dei veicoli a guida assistita si muove nel range fra il secondo ed il terzo livello e, mentre negli ultimi anni si sono iniziati a vedere