PIERPAOLO MARRONE

SPAZI HOBBESIANI?

1. *Cyberspace e cyberwar* 2. *Principi, norme, regole nel cyberspace* 3. *Deterrenza* 4. *Effetto "reputazione" e "rogue State"* 5. *Cyberanarchy* 6. *Hobbes 2.0*

ABSTRACT: *HOBBESIAN SPACES*
In this article I explore some issues related to cyberwar and its implications for the extension of the Hobbesian paradigm of the state of nature to international relations with particular reference to cyberspace. My conclusion is that there are many reasons to believe that this explanatory paradigm should also apply in this area.

1. *Cyberspace e cyberwar*

La guerra che sta infestando l'Europa in questo momento ha sia tutti i tratti di un conflitto tradizionale (movimenti di truppe sul terreno, linee di approvvigionamento, accerchiamenti, bombardamenti stocastici, guerra per il dominio dei cieli, attacchi navali, tecniche di disinformazione)[1] sia le caratteristiche proprie di un conflitto dove le infrastrutture informatiche hanno un peso rilevante anche se difficilmente valutabile. Naturalmente, la guerra è il momento che esalta lo spessore hobbesiano del conflitto potenzialmente permanente nella comunità umana, perché l'idea di Hobbes era che, se lo stato di natura poteva essere neutralizzato grazie all'invenzione della sovranità, ossia grazie alla permanenza di quanto ancora oggi

[1] Cfr. E. Di Rienzo, *Il conflitto russo-ucraino. Geopolitica del nuovo (dis)ordine mondiale*, Rubettino, Soveria Mannelli 2015, per una disamina in chiave di realismo politico degli antecedenti di questo conflitto.

chiamiamo Stato, ben difficilmente questo avrebbe potuto verificarsi al livello delle relazioni tra Stati, che avrebbero continuato a essere governate non dall'invenzione del diritto e dall'esercizio della coercizione legittima, bensì dalla forza[2]. Alcuni addirittura dubitano che il diritto internazionale esista, dal momento che non esiste un sovrano che sia in grado di applicarlo; altri sono fortemente scettici sulla sua possibilità di applicarlo in linea generale a prescindere dai contesti specifici[3].

Esplorerò in queste pagine alcune suggestioni che potrebbero inclinare in favore dell'idea di Hobbes sulla permanenza dello stato di natura nelle situazioni internazionali che riguardano i rapporti tra gli Stati. Lo farò cercando di bilanciare alcune intuizioni, sostenute però dalla letteratura, sulla cosiddetta *cyberwar*[4]. Occorre dire che le posizioni che si confrontano su questo nuovo terreno di scontro tra potenze militari non sono per nulla uniformi. Grosso modo, si può sostenere che ci sono coloro che ritengono che le tecniche di *cyberwar* non escludano il ricorso a strumenti di controllo di diritto internazionale e coloro che ritengono che anche in questo caso il diritto internazionale sia una finzione pronta a crollare al primo accenno di guerra reale e non solo virtuale[5].

Le tecniche di *cyberwar* includono attacchi selettivi ai sistemi informatici degli avversari, attacchi massicci stocastici che

[2] Cfr. T. Hobbes, *Leviatano* (1651), tr. it. Rizzoli, Milano 2011.

[3] Cfr. M. Koskenntemi, *The Gentle Civilizer, The Rise and Fall of International Law*, Cambridge University Press, Cambridge 2001, per una storia e una critica del diritto internazionale; D. Zolo, *I signori della pace. Per una critica del globalismo giuridico*, Carocci, Roma 2001, per una visione conflittuale non-irenica dei rapporti internazionali e della loro codificazione nel diritto internazionale.

[4] Per un primo approccio A. Bonfanti, *Attacchi cibernetici e cyber war: Considerazioni di diritto internazionale*, in «Notizie di Politeia», XXXIV, 132, 2018, pp. 118-127; M. Durante, *Violence, Just Cyber War and Information*, in «Philosophy & Technology», XXVIII, 3, 2015, pp. 369-385; B. Romaya, L. Portmess, *Confronting Cyber Warfare: Rethinking the Ethics of Cyber War*, in «The Journal for Peace and Justice Studies», XXIII, 1, 2013, pp. 44-60

[5] Cfr. R. Dipert, *The Ethics of Cyberwarfare*, in «Journal of Military Ethics», IX, 4, 2010, pp. 384-410 per un confronto tra queste due posizioni.

preparino il campo a successivi attacchi mirati, propaganda elettorale in un paese straniero per favorire determinati candidati e danneggiarne altri, spionaggio industriale, interferenze nelle infrastrutture informatiche civili come, ad esempio, database fiscali, database sanitari, reti elettriche, sistemi di trasporto. Queste tecniche hanno scatenato una escalation di sistemi di protezione dei dati, ai quali, naturalmente, hanno risposto software che bucano questi sistemi. Tale escalation è accolta come normale anche tra l'opinione pubblica, che si è generalmente formata l'opinione che non esista sistema software o database che non possa essere violato.

Secondo finzioni letterarie e cinematografiche molto popolari sarebbe, infatti, sufficiente possedere un accesso a internet e le competenze tecniche necessarie che potrebbero essere acquisite anche da adolescenti *nerd* appena al di qua della soglia dei disturbi sociopatici. Software di paesi potenzialmente ostili, come il celebre anti-virus Kaspersky, vengono passati al setaccio anche in questi giorni nei quali infuria la guerra tra l'Ucraina e la Russia per cercare di capire se contengano *worm* dormienti che possono essere attivati al momento opportuno. Compagnie telefoniche come Huawei, capaci di creare infrastrutture per intere nazioni (tra le quali la posa degli importantissimi cavi sottomarini), vengono bandite dai paesi occidentali, concorrenti della Cina nella lotta per l'egemonia mondiale[6]. Sono questi solo alcuni dei fatti che hanno raggiunto recentemente una dimensione pubblica, i quali contribuiscono a disegnare un mondo di cyberanarchia, saturo di implicazioni disastrose per gli assetti finanziari, per quelli economici, per gli equilibri geostrategici, perché gettano seri dubbi sulle capacità delle democrazie di fronteggiare minacce di questo genere. Uno degli argomenti a sostegno di questa ultima notazione è che le democrazie implicano

[6] Cfr. Yun Wen, *The Huawei Model: The Rise of China's Technology Giant*, University of Illinois Press, Champaign 2020.

per la loro natura di sistemi politici costruiti sulla divisione dei poteri e su sistemi di pesi e contrappesi dai tempi decisionali dilatati. Questi tempi dilatati dalle lungaggini delle procedure mal si adatterebbero a questo nuovo genere di minacce che si possono sviluppare nel giro di pochi minuti o addirittura secondi.

2. *Principi, norme, regole nel cyberspace*

Capirete bene come l'idea di implementare regole obbligatorie per il cyberspazio abbia generato molte perplessità. Non c'è solo il fatto che un'autorità *super partes*, ossia sopra gli Stati, non appare al momento identificabile, ma a questo si aggiunge la questione che nessun Stato ha effettivamente dichiarato di rinunciare volontariamente ai vantaggi competitivi che sono, anche soltanto momentaneamente, generati da una superiorità tattica in potenziali cyber attacchi verso paesi nemici. Non sono certamente mancati i tentativi in questo senso. Ad esempio, l'Organizzazione delle Nazioni Unite ha, su pressioni della Federazione Russa, avviato sin dal 1998 una discussione su "Developments in the Field of Information and Telecommunications in the Context of International Security"[7], come recita il titolo della risoluzione a suo tempo approvata e che avrebbe dovuto portare all'adozione di norme stringenti di sicurezza nel campo delle ICT (Information and Communication Technologies) in caso di guerra. La Svizzera ha implementato un pacchetto di principi per il comportamento responsabile degli Stati nel cyber spazio, che derivano da numerose discussioni che si sono succedute nei vari organismi internazionali e che sono state approvate dall'ONU[8]. Queste sono:

(1) favorire la cooperazione interstatale nel campo della sicurezza informatica;

(2) considerare tutte le informazioni rilevanti;

[7] Cfr. https://www.un.org/disarmament/ict-security/.

[8] https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

(3) prevenire l'uso scorretto delle ICT nel proprio territorio;
(4) pomuovere la cooperazione interstatale per prevenire e reprimere le attività criminali nel cyber spazio;
(5) rispettare i diritti umani e la riservatezza dei cittadini;
(6) non danneggiare infrastrutture critiche di altri Stati;
(7) proteggere le proprie infrastrutture critiche;
(8) rispondere alle richieste di assistenza di altri Stati;
(9) garantire la sicurezza della catena di approvvigionamento per le reti informatiche;
(10) relazionare pubblicamente sulle vulnerabilità alle ICT;
(11) non danneggiare le squadre che rispondono alle richieste di emergenza informatica.

Si comprende bene come questi siano essenzialmente dei principi di buona volontà e non siano affatto delle norme stringenti. La loro stessa indeterminatezza non annuncia la possibilità se non di ulteriori enunciazioni di principio, più che di norme sufficientemente precise. Si prenda l'enunciazione contenuta in (2) che prescrive di considerare tutte le informazioni rilevanti. Il concetto stesso di 'informazione rilevante' è del tutto ambiguo[9], perché un'informazione potrebbe rilevarsi rilevante solo in un tempo successivo indeterminato rispetto al presente, mentre un'altra informazione potrebbe essere ritenuta rilevante e non esserlo affatto. Questa ambiguità interpretativa può essere uno strumento più per non condividere informazioni che per condividerle. Per quanto riguarda l'enunciazione contenuta in (5), questa sembra rimandare alle varie carte dei diritti approvate dagli organismi internazionali[10]. Vi sono, tuttavia, così tanti casi documentati di violazioni di questi diritti da parte di nazioni che li hanno sottoscritti, che la natura di enunciazione di buone intenzioni risulta palese anche in questo caso. Inoltre,

[9] Cfr. L. Floridi, *Understanding Epistemic Relevance*, in «Erkenntnis», LXIX, 1, 2008, pp. 69-92.
[10] Cfr. L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in «Politica & Società», VII, 1, 2018, pp. 61-75.

occorre aggiungere che alcune nazioni non sono affatto in accordo sul contenuto dei diritti umani individuali. La Cina, ad esempio, ha sempre dichiarato che questi devono essere declinati all'interno della sua concezione di diritto umano, dove il diritto individuale è subordinato al benessere collettivo di entità più vaste (sostanzialmente il Partito Comunista Cinese e il suo ruolo nella Cina contemporanea)[11]. Inoltre, è noto che la concezione della riservatezza, mentre ha subito un'evoluzione importante anche nei paesi democratici, ha un tutt'altro significato nei paesi retti da dittature o da sistemi altrimenti autoritari[12]. Per quanto riguarda il principio enunciato in (6), la Federazione Russa stessa che è uno dei paesi all'origine di queste nobili enunciazioni, ha più volte nel corso degli anni lanciato attacchi informatici verso altri paesi, ad esempio l'Ucraina.

Si potrebbe continuare a mostrare la debolezza effettuale di questi 11 principi, ma basti per ora sottolineare il diffuso scetticismo che circonda queste enunciazioni[13]. Questi principi sono anche spesso incorporati in norme che sono ormai parte di codici penali e civili di molte nazioni e lo scetticismo che è possibile esercitare sui primi, si riversa come conseguenza anche sui secondi. Questo scetticismotuttavia potrebbe anche essere il prodotto di una errata interpretazione della funzione delle norme e dei principi. In realtà, di norme e principi noi non possiamo fare a meno[14]. Il fatto che le norme vengano in molteplici circostanze disattese per negligenza oppure violate con intenzioni

[11] Cfr. C. Hamilton, M. Ohlberg, *La mano invisibile. Come il Partito Comunista Cinese sta rimodellando il mondo* (2020), tr. it. Fazi, Roma 2021.
[12] Cfr. L. Yao-Huai, *Privacy and Data Privacy Issues in Contemporary China*, in «Ethics and Information Technology», VII, 1, 2005, pp. 7-15.
[13] Cfr. G. Terzi di Sant'Agata, F. Voce, *Cybersecurity e nuovi equilibri europei e internazionali*, in «Notizie di Politeia», XXXIV, 132, 2018, pp. 99-107; G.R. Lucas, *Postmodern War*, in «Journal of Military Ethics», IX, 4, 2010, pp. 289-298.
[14] Cfr. P.J. Verovsek, *Against International Criminal Tribunals: Reconciling the Global Justice Norm with Local Agency*, in «Critical Review of International Social and Political Philosophy», XXII, 6, 2019, pp. 703-724; C.E. Pavel, D. Lefkowitz, *Skeptical Challenges to International Law*, in «Philosophy Compass», XIII, 8, 2018, pp. 1-14.

criminali da parte di singoli individui o da organizzazioni oppure rese innocue dagli Stati, non significa automaticamente che siano irrilevanti. Può in effetti accadere che una norma ritenuta inapplicabile in determinate circostanze, lo risulti invece quando queste stesse circostanze sono mutate. Se tali norme non fossero state ritenute fungenti in un qualche senso anche quando non era possibile applicarle (o addirittura quando non era consigliabile o conveniente applicarle), allora nessuna autorità potrebbe fare appello alla loro legittimità. Inoltre, non dobbiamo essere vittime dell'ingenuità di pensare che le norme diventino effettivamente applicabili una volta che la procedura corretta per renderle legali sia stata percorsa. Sappiamo che le norme per essere implementate in un sistema legale ed essere riconosciute a livello internazionale devono seguire un percorso lungo e complesso. Le fonti del diritto sonotalvoltadi natura informale e questo significa che la fungibilità di una norma non è affatto un processo governato da automatismi, bensì anche da tutti gli ostacoli, obiezioni, di natura tanto intellettuale quanto comportamentale che una norma vuole eliminare oppure soltanto aggirare. Le norme hanno, insomma, una storia evolutiva, non priva di penombre, spesso governata da meccanismi che non sono, almeno inizialmente, portati alla lucedella deliberazione politica e legislativa[15].

Per quanto riguarda le norme che regolano rapporti tra gli Stati, il tempo della loro gestazione può essere molto lungo. I numerosi trattati per contenere la proliferazione degli armamenti nucleari hanno richiesto molti anni di serrate trattative e di sofisticati compromessi. Le tecnologie informatiche che sono utilizzabili in contesti strategici (ossia potenzialmente tutte) pongono sicuramente dei problemi specifici, dal momento che le dotazioni tecnologiche per condurre un'operazione, ad esempio, di sabotaggio

[15] Cfr. C. Bicchieri, *Norms of Cooperation*, in «Ethics», C, 4, 1990, pp. 838-861.

del sistema elettrico di una nazione sono già disponibili o se non sono attualmente disponibili potrebbero necessitare solo di un nuovo programma che un hacker potrebbe stare già inventando in questo momento. Questo però non è detto sia necessariamente un ostacolo a norme internazionali che si sviluppino per evitare disastri alle infrastrutture informatiche spesso condivise da più Stati.

3. *Deterrenza*

L'applicazione di una norma, di qualsiasi norma, implica anche la capacità di esercitare tanto una deterrenza quanto una minaccia di ritorsione credibili[16]. Questa credibilità può essere resa tale solo da un accordo tra Stati e in particolare nel nostro presente tra Stati Uniti, Unione Europa, Cina, India, Russia. Qualcuno sostiene che la medesima natura di alcuni attacchi informatici rende l'idea della deterrenza qualcosa di completamente diverso da quella che può essere esercitata da nazioni con eserciti o con arsenali nucleari[17]. Ma anche in questo caso, sostengono i fautori delle regole, non ci sono alternative per ridurre il rischio se non l'uso congiunto di diplomazia, deterrenza, minaccia. Non sempre però è chiaro quale possa essere la deterrenza che si può usare verso un ristretto gruppo di cyber criminali, magari asserragliati in qualche remota regione montuosa dell'Afghanistan o capaci di rendersi irreperibili nel cyber spazio. La nozione stessa di cyber spazio implica il riconoscimento che in questo spazio, lo spazio dell'informazione, non ci sono confini nazionali. Allo stesso tempo è difficile tracciare i confini tra ciò che costituisce una minaccia per il pubblico e ciò che costituisce una minaccia per un privato, si tratti di un individuo oppure di una compagnia commerciale o di una industria. Questo

[16] Cfr. J.-P. Dupuy, *On the Rationality and Ethics of Nuclear Deterrence*, in «Philosophical Journal of Conflict and Violence», V, 1, 2021, pp. 135-138.
[17] Cfr. M. Taddeo, *Deterrence by Norms to Stop Interstate Cyber Attacks*, in «Minds and Machines», XXVII, 3, 2017, pp. 387-392.

potrebbe portare a allargare i limiti di intervento dello Stato negli spazi che attualmente vengono riconosciuti come dominio esclusivo dell'individuo (ammesso che in questo momento tali limiti siano sempre chiari)[18]. Inoltre, almeno nelle democrazie la sicurezza anche di compagnie industriali che costituiscono asset strategici per gli Stati dove sono insediate non è ritenuta finora pertinenza esclusiva dello Stato, ma viene lasciata all'iniziativa della compagnia medesima. Questo potrebbe essere considerato bizzarro. In fin dei conti, se la possibilità di una rapina in banca impone alle forze dell'ordine di intervenire con iniziative repressive preventive, non si capisce perché questo non dovrebbe essere ritenuto indispensabile anche nel caso di furti di segreti industriali. Non tutte le filiali bancari si dotano di personale di sicurezza, come è evidente dall'esperienza di ognuno. Questo accade perché la capacità di minaccia e deterrenza dello Stato è ritenuta sufficientemente solida.

La reputazione dello Stato come agente coercitivo può talvolta essere sufficiente a limitare gli investimenti stessi nella sicurezza, quando si tratta di minacce di aggressioni agli individui o di furti di proprietà fisiche. Ma nel caso di beni che si trovano nella cosiddetta infosfera, le cose sembrano complicarsi, anche per il fatto che ho ricordato che una difesa inadeguata da parte di compagnie private può avere importanti effetti su vasti settori di interesse pubblico, mentre questo effetto è in linea di principio più limitato, ad esempio, nel caso di una rapina o di un furto in un'abitazione privata. Come si dice tra chi si occupa di strategia, il cyber spazio è divenuto il quinto territorio, dopo la terra, il mare, l'aria, lo spazio extraterrestre dove i conflitti sono combattuti[19]. Molte nazioni si sono oramai dotate non solo di corpi di polizia specializzati

[18] Cfr. L. Floridi, *Four Challenges for a Theory of Informational Privacy*, in «Ethics and Information Technology», VIII, 3, 2006, pp. 109-119.
[19] Cfr. F. Rugge, *'Mind Hacking': La guerra informativa nell'era cyber*, in «Notizie di Politeia», XXXIV, 132, 2018, pp. 108-117.

nel riconoscimento dei crimini informatici, ma anche di settori degli eserciti nazionali che si occupano precipuamente della guerra informatica[20]. Mentre nel recente passato si immaginava che un conflitto che vedesse la presenza di un attore nucleare avrebbe potuto essere iniziato dallo scoppio di un ordigno nucleare a basso potenziale per mettere fuori uso tutti gli apparecchi elettronici in un'area circoscritta, ora questa sembra essere una nozione desueta, superata dalla possibilità di raggiungere il medesimo obiettivo attraverso un cyber attacco, che potrebbe essere di difficile o impossibile individuazione quanto all'origine e quanto all'autore.

Ciò che si sottolinea spesso, anche relativamentealla possibilità di introdurre norme e erogare sanzioni nel caso di azioni ostili, è che le azioni di guerra informatica non hanno la stessa pregnanza delle azioni militari vere e proprie, perché non implicano l'uso di truppe sul terreno, o di missili lanciati verso obiettivi militari o civili, o l'utilizzo di forze navali per bloccare un porto. Del resto, ci sono da qualche parte numeri assoluti sulle vittime causate da cyber attacchi? Le attività di cyber war sarebbero quindi parassitarie, soprattutto nel caso di guerre e azioni ostili di Stati nei confronti di altri Stati, rispetto ad altre attività sul terreno[21]. Lo stesso però si potrebbe probabilmente dire di attività compiute da singoli o d gruppi criminali. Anche queste sono attività che vengono svolte non per il gusto di farle (a meno che non siano compiute da qualche nerd narcisista), bensì per ottenere dei profitti. Inoltre, azioni cyber per scopi politici possono essere compiute anche da gruppi terroristici che non hanno necessariamente dei legami con Stati. Quello che ancora non risulta chiaro è però che cyber attacchi da parte di Stati potrebbero generare le dinamiche

[20] Cfr. D.J. Lonsdale, *The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios*, in «Journal of Military Ethics», XIX, 1, 2020, pp. 20-39.

[21] Cfr. E. Barrett, *Warfare in a New Domain: The Ethics of Military Cyber-Operations*, in «Journal of Military Ethics», XII, 1, 2013, pp. 4-17.

tipiche dell'escalation e portare a un conflitto sul terreno. Forse, tutto questo però non è difficile da immaginare. Tutte le forze armate degli Stati dipendono in maniera stretta da infrastrutture civili che non sono prevalentemente adibite a uso militare, con l'unica eccezione delle basi militari. Sono queste infrastrutture i bersagli degli attacchi informatici. I danni che possono essere arrecati con questi attacchi possono risultare molto rilevanti. Si pensi a un attacco informatico che riesca a spegnere gli impianti elettrici degli ospedali e che sia propedeutico a un attacco militare tradizionale. Un attacco del genere potrebbe danneggiare la rete logistica delle forze di difesa[22].

Prima dell'invasione terrestre dell'Ucraina da parte della Federazione Russa, sono stati compiuti numerosi attacchi informatici nel corso degli anni. È chiaro che molti tra questi hanno avuto lo scopo di saggiare il livello di sicurezza dell'Ucraina, oltre a creare danni per svariati miliardi di dollari. Con la diffusione dell'internet delle cose, l'utilizzo sempre più massiccio e pervasivo dei big data, di elettrodomestici collegati alla rete, il prossimo utilizzo di esoscheletri a uso militare e medicale, qualsiasi apparato collegato al web potrà essere oggetto di un attacco informatico. Gli attacchi sono quindi destinati a aumentare in maniera esponenziale. La storia del cyber crimine e delle operazioni militari o di spionaggio militare e/o industriale coincide del resto quasi perfettamente con la storia di internet. I primi attacchi informatici si fanno risalire agli inizi degli anni Ottanta del secolo scorso[23]. Proprio l'aumento impressionante, ma prevedibile, degli attacchi informatici dovrebbe indurre a ripensare il concetto di deterrenza e la funzione delle norme, sostengono quelli che non sono scettici

[22] Cfr. D. Whetham, *"Are We Fighting Yet?" Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?*, in «Monist», XCIX, 1, 2016, pp. 55-69.
[23] Cfr. B. Middleton, *A History of Cyber Security Attacks. 1980 to Present*, Auerbach Publications, New York 2017.

sull'implementazione di principi e norme di regolazione e repressione.

C'è un'ovvia differenza tra la deterrenza nucleare, racchiusa nell'acronimo MAD (Mutual Assured Distruction)[24] e la deterrenza che è esercitata verso chi commette crimini informatici. Nel primo caso la deterrenza è la minaccia credibile esercitata per evitare un evento singolo. Infatti, nel caso di un attacco nucleare con conseguente *retaliatation*, con tutta probabilità non ci sarebbe una terza mossa. Nel secondo caso, questa è spesso paragonabile alla consueta attività preventiva delle forze dell'ordine. Questa attività preventiva non si esaurisce nella minaccia credibile di attività repressive, ma comprende anche attività educative presso la popolazione generale per renderla consapevole di attività che potrebbero avere dei profili penali. Il problema naturalmente è che, se questa è effettivamente una delle funzioni delle norme, individui e gruppi criminali non se ne fanno certo impressionare, soprattutto quando è possibile commettere dei reati con la quasi certezza di non essere presi. Questo non significa affatto però che la deterrenza non abbia un significato importante per prevenire cyber attacchi da parte degli Stati. Il fatto è che questa deterrenza non può essere esercitata solo attraverso gli strumenti informatici. Infatti, gli Stati Uniti hanno dichiarato ripetutamente che a un cyber attacco si riservano di rispondere attraverso strumenti di propria scelta[25]. La risposta è chiara ed è stata efficace, almeno a giudicare da quanto finora, a nostra conoscenza, non è successo. Non si sono verificati a oggi attacchi alle infrastrutture statunitensi tali da causare danni visibili su larga scala.

[24] Cfr. T.W. Luke, *The Discourse of Deterrence: National Security as Communicative Interaction*, in «Journal of Social Philosophy», XXI, 1, 1991, pp. 30-44.

[25] Cfr. C.L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, The George Washington University, Cyber Security Policy and Research Institute, Report GW-CSPRI-2011-5, 2011.

La deterrenza è perciò costituita in questo ultimo caso dalla capacità di utilizzare mezzi militari convenzionali e dalla proclamata intenzione di poter trattare anche episodi di spionaggio come attacchi militari. Se la capacità di deterrenza è reale, allora l'iniziativa è lasciata in situazioni asimmetriche nelle capacità di chi la possiede. Anche nel caso di confronto tra potenze, tuttavia, una combinazione di questi fattori può influenzare le strategie di confronto, inducendo a un più attento calcolo dei costi e dei benefici di un attacco informatico. La proposta che era stata avanzata dalla Federazione Russa di bandire tutti gli strumenti di guerra elettronica assomigliava perciò più a una boutade propagandistica che a una proposta concreta e mirava a provocare una risposta negativa degli Stati Uniti. La Cina nel frattempo rimaneva silente e i motivi sono del tutto chiari. Questi motivi sono legati sia al progetto cinese di egemonia in campo internazionale sia ai sistemi di controllo interno che si avvalgono massicciamente, almeno nelle città, di strumenti di controllo informatico della popolazione sia ai fini dell'implementazione del cosiddetto sistema di "credito sociale" sia per monitorare l'utilizzo dei social sia per controllare il flusso delle notizie.

4. *Effetto "reputazione" e "rogue State"*

L'ONU non ha accolto la demagogica proposta russa, ma ha istituito numerosi gruppi di confronto tra Stati membri. Alcuni hanno raggruppato un numero ristretto di rappresentanze diplomatiche, mentre altri erano aperti al contributo di chiunque. Il risultato è stata la formulazione di quei principi che ho ricordato all'inizio e che sono stati adottati da alcuni Stati. A fondamento di questi principi sta però un principio generale ossia che il diritto internazionale è alla base di questi principi che vengono volontariamente e in maniera non vincolante adottati dagli Stati membri che lo desiderano. Il fatto che siano adottati

volontariamente e su base non vincolante riflette semplicemente una caratteristica del sistema stesso del diritto internazionale che non può essere considerato analogo al diritto penale, civile, amministrativo adottato da uno Stato[26]. In questo caso, principi, norme, regole hanno valore vincolante. Tuttavia, se pur si deve riconoscere l'importanza di aver statuito questi principi non vincolanti e assumibili solo su base volontaria, rimane l'ambiguità di alcuni tra questi. Questa ambiguità non è tanto nel modo nel quale i principi sono stati enunciati né nella loro sostanza, bensì piuttosto nella natura delle cose. Ad esempio, il principio che non devono essere attaccate le infrastrutture civili è apparentemente molto nobile, ma completamente inattuabile, dal momento che, come si ricordava, le capacità militari di uno Stato dipendono dall'utilizzo massiccio di infrastrutture civili. In caso di conflitto, ad esempio, le strade sono uno strumento militare e così porti, aeroporti e ferrovie, tutte strutture che dipendono in larga parte da sistemi informatici. Anche i gruppi di discussione che si sono costituiti come panel aperti a chi volesse fornire un contributo, con l'ausilio di Ong e compagnie private non hanno elaborato proposte maggiormente articolate di quella che proponeva gli 11 principi non vincolanti. Ci si è limitati a ribadire la rilevanza del diritto internazionale per le attività nel cyber spazio. Nulla più di una tautologia rispetto a quanto già precedentemente eleborato e probabilmente non poteva essere altrimenti[27].

Altri panel internzionali di discussione hanno proposto l'introduzione di norme maggiormente specifiche, come la proibizione di utilizzare bot per entrare nei sistemi informatici civili degli Stati. Questo equivarrebbe sostanzialmente al divieto

[26] Cfr. F.V. Kratochwil, *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*, Cambridge University Press, Cambridge 1989.

[27] Cfr. S. Pietropaoli, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in «Rivista di filosofia del diritto», VIII, 2, 2019, pp. 379-399.

di lanciare attacchi informatici, che è appunto quanto su cui si sta discutendo. L'introduzione di norme maggiormente specifiche può però essere di notevole importanza perché segnala il meccanismo evolutivo presente anche nel caso di principi, norme, regole, che partendo da enunciazioni generali si specifica via via maggiormente. Tuttavia, c'è anche un rischio che deve essere segnalato. Dal momento che si sta trattando di un campo dove le innovazioni tecnologiche si susseguono a un ritmo molto rapido, l'introduzione di una eccessiva specificazione potrebbe essere semplicemente inutile, perché superata nei fatti. Principi, norme, regole hanno un ritmo di implementazione molto più lento di quanto avviene nelle realtà che ci si propone di regolamentare. Questo, del resto, è coerente con la loro natura di strumenti *ex post*. Preoccupazioni ulteriori vengono dalla possibilità di conseguenze non previste nell'utilizzo di attacchi informatici. Questi potrebbero essere lanciati con l'idea di saggiare le capacità di reazione dell'antagonista, ma potrebbero avere conseguenze non intenzionali di portata ben maggiore, provocando così un'escalation[28]. Proprio per questo, alcuni pensano che potrebbero essere sottoscritti trattati analoghi a quelli sulle armi nucleare, ad esempio per limitare l'uso di alcune risorse informatiche. Non è però chiaro quali dovrebbero essere queste risorse. Si dovrebbe limitare l'uso dei supercomputer limitandone la potenza di calcolo? Sembra un'ipotesi del tutto irrealistica per molti motivi. Innanzitutto perché è probabile che una potenza di calcolo sempre maggiore sarà necessaria per integrare le infrastrutture civili tra di loro. In secondo luogo, questa stessa potenza potrebbe essere necessaria per elaborare strumenti di difesa informatica sempre più sofisticati per poteggersi da minacce anch'esse sempre più sofisticate.

[28] Cfr. L. Carlson, R. Dacey, *Social Norms and the Traditional Deterrence Game*, in «Synthese», LXXIV, 1, 2010, pp. 105-123.

Molte risorse informatiche sono in mano a aziende private in quella parte di mondo dove prevalgono le democrazie rappresentative e le economie di mercato. Non è detto che questa situazione possa continuare nel futuro. Alcune risorse informatiche sono già considerate strategiche per la sicurezza degli Stati e tutti gli Stati possiedono norme sufficientemente elastiche da poter includere rapidamente alcuni settori all'interno di quelli che devono essere supervisionati perché cruciali per la sicurezza nazionale. Lasciando da parte per ora il caso di Stati dove questa supervisione è ben presente, come è il caso della Cina, dove tutte le compagnie di un determinato peso sono considerate potenzialmente strategiche e sono partecipate da organismi riconducibili al Partito Comunista Cinese, anche i governi democratici potrebbero voler controllare le compagnie private che hanno interessi e/o potenzialità in materia di sicurezza. Già ora in alcuni Stati alle compagnie private non è possibile rispondere attivamente con atti di rappresaglia ad attacchi malevoli.

Nell'ambito dell'evoluzione delle norme può giocare un ruolo il cosiddetto "effetto reputazione". Essere considerato un "rogue State" ha degli effetti non soltanto reputazionali, bensì economici e potrebbe minare la stabilità dell'assetto interno di certi Stati. Ci sono strumenti bellici che sono banditi dai trattati internazionali, come armi chimiche e biologiche. Questo non significa affatto, come è facilmente immaginabile, che alcuni Stati non le stiano sviluppando o non ne possiedano depositi significativi. Tuttavia, tutto questo non può essere fatto pubblicamente alla luce del sole, perché provocherebbe sanzioni e altri atti ostili da parte delle potenze che se ne dovessero sentire minacciate. Qualcosa del genere potrebbe forse essere immaginato nel caso di Stati che utilizzassero compagnie private per effettuare "proxy cyberwars" (guerre informatiche per

procura)[29]. Il danno alla reputazione internazionale di uno Stato talvolta si misura anche sulla possibilità, concreta o propagandata, di causare un alto numero di vittime tra la popolazione civile con armamenti banditi dalle convenzioni internazionali, come è il caso di armi chimiche, biologiche, nucleari, o di armi convenzionali come bombe al fosforo, a grappolo, o particolari mine antiuomo. Nel caso di queste armi ci si può ben e facilmente immaginare che alti esponenti di uno Stato si presentino nei consessi internazionali esibendo foto di installazioni missilistiche ritenute una minaccia imminente alla propria sicurezza, come accadde nella crisi di Cuba del 1962, o esibendo presunte prove della fabbricazione di armi di distruzione di massa, come accadde prima dell'invasione americana dell'Iraq. Difficile immaginare qualcosa di simile nel caso di un attacco informatico. È irrealistico credere che esponenti di alto rilievo ottengano attenzione mediatica, di solito necessaria prima di un intervento militare sul campo, esponendo pubblicamente parti di un codice. Inoltre, le intrusioni in sistemi informatici dotati di alte soglie di protezione spesso suscitano ammirazione perché la scrittura di codici malevoli è ritenuta un'abilità esoterica riservata a pochi. A ciò si aggiunga che di solito queste intrusione non suscitano immediatamente delle vittime militari e/o civili, come accade nel caso di un attacco militare. Si potrebbe però pensare che il principio che vieta di attaccare infrastrutture civili come gli ospedali riguardi anche le sue strutture informatiche. In questo caso, forse, l'effetto reputazione potrebbe essere analogo a quello che colpisce *rogue State* che usano armi bandite dalle convenzioni internazionali. D'altra parte, proprio l'alta interconnessione delle strutture della rete informatica potrebbe rendere difficile da capire se l'obiettivo principale di un attacco è, poniamo, un'infrastruttura

[29] Cfr. J. Collier, *Proxy Actors in the Cyber Domain: Implications for State Strategy*, in «St. Antony's International Review», XIII, 1, 2017, pp. 25-47.

sanitaria, oppure se il danno che a questa è stato causato sia un effetto collaterale non previsto e non intenzionale.

5. *Cyberanarchy*

Non è affatto chiaro come potrebbe funzionare un trattato per un uso limitato di strumenti informatici da usare in caso di attacco o di difesa[30]. Al momento attuale, gli attacchi hanno, per quanto se ne sa, anche nel caso di conflitti armati, riguardato infrastrutture connesse con obiettivi militari o finanziari. Nel caso di attacchi a infrastrutture civili, come il recente attacco contro le Ferrovie dello Stato italiane, l'intenzione malevola sembra essere quella di ottenere un riscatto per sbloccare il sito che è stato hackerato. Che dietro questo attacco ci sia uno Stato ostile (il nome che è stato fatto è naturalmente quello della Federazione Russa) non è certo. Potrebbe essere che questo o altri attacchi siano stati pilotati da Stati e che le intelligence dei paesi colpiti ne siano a conoscenza con ragionevole certezza, ma non vogliano propagandarlo per non innescare una escalation. Come si diceva, c'è apparentemente un consenso vasto sulla necessità di regolamentare il cyber spazio proprio per evitare possibili escalation, Ma dove si debba precisamente tracciare i limiti che potrebbero condurvi è una materia del tutto controversa.

Coloro che sono scettici sulla portata e effettualità del diritto internazionale traggono uno dei loro recenti argomenti proprio dall'anarchia del cyber spazio[31]. Ad esempio, già dal 2015 gli Usa e la Cina hanno convenuto sulla necessità di non usare strumenti di spionaggio informatico per acquisire vantaggi commerciali. Questo accordo è stato però largamente disatteso, proprio in ragione di altre circostanze politiche e economiche. È da dubitare, inoltre, che uno Stato che è la potenza antagonista

[30] Cfr. J. Goldsmith, *Cybersecurity treaties. A Skeptical View*, https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf.

[31] Cfr. L. Lessig, *The Zones of Cyberspace*, in «Stanford Law Review», XLVIII, 5, 1996, pp. 1403-1411.

degli Usa possa e voglia distinguere tra condizioni politiche e condizioni economiche. Principi, norme, regole devono innanzitutto venire a patti con il suo disegno egemonico. Che cosa precisamente è un atto di spionaggio commerciale in quanto distinto da un atto di spionaggio militare? Che cosa è un atto di spionaggio politico in quanto distinto da un atto di spionaggio commerciale e politico? È chiaro che, ad esempio, un atto di spionaggio politico potrebbe tradursi in un vantaggio commerciale. Queste attività si intersecano tra di loro e spesso semplicemente non è possibile distinguerle. I trattati internazionali rappresentano la constatazione di un'area grigia mascherata dall'assertività dei principi. D'altra parte, è forse proprio questa area grigia a consigliare molte volte di non violarli. Quello che intendo dire è che violare o non violare un trattato, un accordo, una dichiarazione di intenti, ammesso sia chiaro sia avvenuto e chi sia a averlo commesso, è una questione di calcolo delle utilità attese e non di adesione a principi. Il problema non è quello di aderire a dei principi, ma di rendere sconveniente violarli troppo liberamente[32]. Tuttavia, il problema rimane sempre quello, ossia l'erogazione della pena individuato il colpevole. Questo non può avvenire attraverso uno Stato sovranazionale, che al momento né esiste né è all'orizzonte remoto, bensì solo attraverso gli strumenti che le potenze planetarie hanno già nelle loro disponibilità. Sembra un banale truismo, ma mette in chiaro che principi, norme, regole seguono il flusso della potenza politica e del calcolo delle utilità. Questo vale a dimostrare l'integrazione di queste attività ostili sia nella competizione costante tra gli Stati sia nelle attività potenziali sul campo di battaglia. Il Cyber Command degli Usa adotta, infatti, la strategia del "persistent engagement" che è la medesima costantemente utilizzata

[32] Cfr. J. Goldsmith, *Against Cyberanarchy*, in «The University of Chicago Law Review», LXV, 4, 1998, pp. 1199-1250.

dalla fine della seconda guerra mondiale[33]. Il *persistent engagement* ha numerosi vantaggi, e principalmente due: l'esercizio costante della pressione sulle infrastrutture di Stati potenzialmente ostili, come dimostrano anche i sabotaggi di Israele al programma nucleare iraniano; la flessibilità nella scelta della risposta che non è vincolata a un sistema preciso di norme.

I trattati internazionali sugli armamenti possono contenere anche delle liste che specificano quali comportamenti dovrebbero essere considerati degli incidenti. Questo accade già anche in altri campi, ad esempio in campo navale. Si ripropongono probabilmente qui i medesimi interrogativi che si sono incontrati altre volte in queste pagine, poiché mentre è più facilmente verificabile nella realtà non virtuale cosa possa essere definito come incidente, questo può risultare difficile nel cyber spazio. Se una nave o un aereo da combattimento hanno un'avaria, che magari coinvolge anche i tradizionali sistemi di comunicazione via radio, potrebbero però segnalare in altro modo le proprie intenzioni non ostili quando sconfinano in territori potenzialmente ostili. Ma nel caso del cyber space non è affatto chiaro come questo possa avvenire. Forse comunicando tempestivamente le proprie intenzioni e fornendo codici potenzialmente dannosi? D'altra parte un codice potenzialmente dannoso per l'avversario costituisce un chiaro vantaggio competitivo e quindi non si capisce perché condividerlo, se non in presenza della minaccia credibile di una ritorsione. C'è una difficoltà ulteriore riguardo a trattati internazionali per limitare l'uso di strumenti di cyber attacco, che si può desumere dalla storia delle numerose trattative Usa-Urss per limitare gli armamenti nucleari. In quel caso, erano previsti strumenti di controllo per verificare l'applicazione dei trattati. Ad esempio, commissioni che si riunivano periodicamente per verificare il

[33] Cfr. M.P. Fischerkeller, R.J. Harknett, *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation*, in «The Cyber Defence Review», IV, 2019, pp. 267-287.

progresso nell'applicazione dei trattati, ispezioni periodiche nei siti di interesse, possibilità di voli di ricognizione sui siti di interesse e così via. Nel caso della prevenzione di cyber attacchi è difficile per il momento anche immaginare quali potrebbero essere questi strumenti di controllo e di prevenzione. Nel caso di incidenti il controllo e la verifica potrebbero essere ovviamente solo ex post e potrebbero certamenteavere una decisa utilità per prevenire l'occorrenza di incidenti futuri. Ma nel caso di verificare le buone intenzioni delle parti in causa di aderire a un trattato che cosa bisognerebbe fare? Ispezionare i siti dove risiedono i server governativi e i programmi che vi sono installati? Questo però potrebbe facilmente trasformarsi in un'operazione di spionaggio. Lanciare dei bot con funzioni di sorveglianza, allora? Anche in questo caso potrebbero riproporsi le stesse difficoltà.

6. *Hobbes 2.0*

Si dirà che queste obiezioni riguardano difficoltà legate alla tecnica e perciò non si tratta di difficoltà insormontabili in linea di principio. Questa è una linea argomentativa seria ed è di fatto presupposta da tutte le proposte che sono state avanzate in questo campo per prevenire cyber attacchi e cyber incidenti. Anche gli incontri, precedenti alla guerra in corsoin Europa, tra Federazione Russa e Usa sono state avanzate delle proposte per delimitare precisamente le infrastrutture che non dovrebbero in nessun caso essere oggetto di cyber ostilità. Tra questeil presidente Biden ha proposto le infrastrutture comunicative, l'energia, i servizi finanziari, e le stesse ITC, almeno a leggere i resoconti della stampa. Questa lista sembra però essere più un'operazione di propaganda che una concreta proposta operativa. D'altra parte, spesso accordi importanti sono iniziati proprio con queste modalità comunicative. Biden ha aggiunto che gli Usa possiedono gli strumenti necessari per attuare delle rappresaglie

in caso di attacchi a queste strutture. Si potrebbe anche speculare che le aree che non sono state nominate siano perciò oggetto possibile di cyber attacchi che non comporterebbero rappresaglie, mafrancamentecredo che la logica sia di scarso aiuto per trarre ragionevoli conseguenze in questo campo.

Le guerre informatiche hanno talvolta l'aspetto di guerre per procura combattute da mercenari informatici. È facile immaginare che dietro a questi mercenari informatici spesso ci siano dei governi, poiché è ovvio che anche soltanto per intervenire in attività di spionaggio sulle dorsali informatiche sottomarine che trasportano i cavi di fibra ottica sono necessari degli investimenti che unicamente uno Stato è in grado di fare. Tuttavia, ci sono delle ragioni per non essere completamente pessimisti sulla formulazione di principi, regole, norme in ambito internazionale. Innanzitutto, la loro formulazione e sottoscrizione segnala che esiste un accordo che coinvolge più parti. Questo non è realisticamente sufficiente. Anche la Corte Penale Internazionale ha visto l'adesione di numerosi Stati, ma non vi aderiscono, tra gli altri, Usa, Cina, Russia. Certamente questo non è un motivo necessario per non proseguire nel suo lavoro. Appellarsi a trattati sottoscritti giustifica e rende credibile atti di limitata rappresaglia. Al solito, la possibilità di accedere a una minaccia deve essere credibile, ma implementare pubblicamente delle norme sembra essere un passo necessario preliminare alla rappresaglia, almeno se non si è un *rogue State*. Si potrebbe pensare che la rappresaglia non sia solo un atto di forza, ma possa consistere in atti dissuasivi credibili. Si potrebbe immaginare che alcune norme maggiormente stringenti siano fungenti per paesi alleati (Unione Europea e Nato) e altre meno stringenti per altri paesi e che alle prime siano associati benefici per i contraenti. Quanti più Stati di rilievo strategico sottoscrivono norme del genere, tanti più saranno propensi a erogare sanzioni o a limitare la cooperazione nei riguardi di

altri Stati, che invece non li sottoscrivono. Tutto questo sta accadendo in numerosi campi delle relazioni tra gli Stati e non certo da oggi. Che questo sia sufficiente a rendere inadeguata la notazione di Hobbes che le relazioni tra Stati riproducano lo stato di natura è per ora un *wishful thinking*.

Pierpaolo Marrone insegna Filosofia morale presso l'Università di Trieste
marrone@units.it