La *"Cyberwar"*. Le sue modalità e gli strumenti giuridici per contrastarla

di Guido Valenti

Abstract: *Cyberwar. Its modalities and legal tools to respond to it* - This paper analyzes the growing threat posed by cyberattacks and the responses to them provided by domestic and international law. It will first focus on the reasons for the increasing prevalence of cyberattacks, their definition, and their features. It will then analyze the relative U.S. legal framework, considering the separation of war powers between the President and Congress. Finally, it will try to determine when a cyber-attack may allow a response in self-defense under Article 51 of the U.N. Charter. The paper will conclude, given the rising threats, by emphasizing the need for a new treaty to regulate the matter.

Keywords: Cybernetic warfare; US legal framework; Covert action statue; U.N. Charter; Self-defense.

1. La crescente minaccia della guerra cibernetica

Il cyberspazio rappresenta il più recente "*ambiente di guerra*", andando ad integrare il cosiddetto "quinto dominio", dopo terra, mare, cielo e spazio.

Il ricorso da parte degli Stati belligeranti (e non) agli strumenti cibernetici, sin dal loro primo impiego "ufficiale" nella Seconda guerra dell'Ossezia del Sud (2008)[1], è cresciuto esponenzialmente (di pari passo con la loro efficacia), trasformandoli da semplici mezzi di supporto per le tradizionali operazioni di guerra cinetica a delle vere e proprie armi cui vengono dedicate apposite (e sempre più articolate) strutture militari dai vari paesi[2].

[1] Per un'analisi più approfondita si rinvia a: N. Taddei, *"Cyberwar lo strumento bellico del futuro? Il caso Russo-Georgiano"*, in *Centro di Studi Strategici, Internazionali e Imprenditoriali*, 2015, e J. Markoff, *"Before the Gunfire, Cyberattacks"*, *NewYork Times*, 12 agosto 2008.

[2] A titolo meramente esemplificativo si ricordano le vicende che hanno portato, nel corso di sette anni (2010-2017) ed attraverso diverse risoluzioni governative, alla nascita ed al rafforzamento dell'apparato di cyberdifesa dello Stato di Israele. Tutto inizia con la creazione, fortemente voluta dall'allora Primo Ministro Netanyahu, della *"National Cyber Initiative"* (2010), ossia di un comitato di esperti espressamente incaricato di: esaminare lo stato della cybersicurezza in Israele e di elaborare una politica per la nazione che fosse in grado di proiettarla in una posizione di egemonia globale entro il 2015. Dopo aver recepito con la risoluzione n°3611/2011 le raccomandazioni della *"National Cyber Initiative"*, il governo israeliano ha intrapreso un programma volto a centralizzare e riformare il proprio apparato di cyberdifesa (fino ad

DPCE online
ISSN: 2037-6677

Tale tendenza, in continuo sviluppo e dagli esiti difficilmente prevedibili, può essere spiegata ricordando come l'informatica rappresenti lo strumento ideale per la conduzione delle cosiddette "guerre ibride" e ciò per tre ragioni fondamentali[3].

Anzitutto le operazioni di *cyberwarfare* comportano, per chi le voglia intraprendere, dei costi molto ridotti. I *software* utilizzabili a scopi militari sono facilmente producibili e commercializzabili (si pensi al caso della società *"Hacking Team"* che, situata in un appartamento di Milano, produceva software RCS utilizzati anche, ma non solo, dai regimi dittatoriali di Sudan, Libia ed Etiopia per controllare i propri oppositori politici[4]) e molto spesso è sufficiente la semplice modifica (o l'uso in modo illecito) di programmi già sviluppati per l'uso civile. Inoltre, le operazioni di guerra cibernetica non impongono il ricorso a grandi e complesse strutture organizzative, potendo essere efficacemente condotte da uno sparuto gruppo di specialisti (o anche da un singolo individuo) e pertanto risultando facilmente accessibili anche agli stati più poveri.

La seconda ragione del successo dei *cyber* attacchi risiede nella loro versatilità, in quanto essi consentono di colpire i bersagli nemici in qualunque luogo ed in ogni momento garantendo, al contempo, l'anonimato pressoché assoluto dell'aggressore.

Infine, si ricorda come le operazioni di *cyberwarfare* stiano acquisendo, nel contesto di una società sempre più informatizzata, un potenziale distruttivo dirompente. Del resto, il livello di sicurezza generale di un sistema informatico (specie se altamente complesso ed interconnesso come quelli odierni) deve essere parametrato sulla base di quello della sua componente più debole, la cui corruzione o distruzione (dovuta ad un mancato aggiornamento, alla presenza di sistemi operativi obsoleti, o ad una semplice distrazione umana) può portare al crollo dell'intero sistema determinando ingenti danni fisici ed anche la perdita di vite umane[5].

Così, si pensi all'esempio fortemente evocativo del *malware* che (infiltratosi attraverso una *spam* distrattamente aperta da uno dei suoi operatori, o diffuso da un agente nemico tramite un supporto *USB*) riesce a

allora strutturatosi sulla base di una serie di provvedimenti *ad hoc* e dunque dalla natura piuttosto caotica), ma anche ad incentivare la cooperazione tra l'amministrazione statale e le principali aziende del settore. Il percorso si è concluso nel 2017 quando, dopo la definitiva unificazione degli apparati di cyberdifesa interni alle forze armate, si è istituito (con la risoluzione n°3270/2017) l'*"Israel National Cyber Directorate"*, agenzia governativa responsabile della gestione di tutti gli aspetti della cyberdifesa civile e posta, come il Mossad, sotto il diretto controllo del Primo Ministro. Per una ricostruzione più approfondita si rinvia a L. Tabansky, *"Israel Defense Forces and National Cyber Defense"*, in 19 *Connections: The Quarterly Journal* 1, 2020, 45 ss. e J. Frei, *"Israel's National Cybersecurity and Cyberdfense Posture"*, in *CSS Cyberdefense Reports*, 2020;

[3] Sul punto si rinvia a M.G. Losano, *Guerre Ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forini, T. Vettor (a cura di), *Sicurezza e libertà in tempo di terrorismo globale*, Torino, 2017, 19 ss.

[4] Per una completa ricostruzione dei fatti si rinvia a R. Meggiato, *"Cyberwar"*, Milano, 2016, 179 ss. e M.G. Losano, *"Guerre Ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto"*, cit.

[5] Sul punto si rinvia a S.R. Soare, J. Burton, *Smart Cities, Cyber Warfare and Social Disorder*, in *NATO CCDCOE*, 2020, 115.

corrompere il sistema di controllo di una diga, determinandone l'improvvisa apertura e provocando in pochi attimi un'inondazione su vasta scala.

Benché gli scenari aperti da questa nuova tipologia di conflitti fossero già stati prospettati ed analizzati, è solo dal luglio del 2010, con la rivelazione dell'operazione *Stuxnet*, che la concreta minaccia posta dai cyberattacchi ha assunto un ruolo di primo piano nelle agende politiche di tutto il mondo. Il *malware* (la cui origine, nonostante i forti sospetti sul coinvolgimento delle intelligence statunitense ed israeliana, resta ancora ufficialmente ignota) riuscì ad infettare in poco tempo la gran parte del sistema informatico iraniano, ma produsse i suoi effetti solo sui *software* che controllavano le centrifughe della centrale di arricchimento nucleare di Natanz, provocandone il sovraccarico e portando al blocco dell'intero impianto[6]. La comparsa della prima *"precision-guided cyber weapon"*, rivoluzionando la moderna nozione di vulnerabilità delle infrastrutture critiche[7], ha determinato una crescente corsa agli armamenti cibernetici e l'elaborazione di piani strategici sempre più articolati e complessi, nei quali i profili della difesa e dell'attacco preventivo finiscono inevitabilmente per confondersi e per delineare esiti tutt'altro che rassicuranti (come dimostra plasticamente il concetto di *"defend forward"*, elaborato nel 2018 dallo *US Cyber Command*)[8].

Il crescente pericolo posto dai cyberattacchi e le conseguenti reazioni dei governi dei diversi paesi spingono a chiedersi quale sia il regime giuridico (sia all'interno dei singoli ordinamenti nazionali, sia al livello del diritto internazionale) deputato a disciplinare la materia e quali soluzioni esso possa offrire allo Stato che intenda reagire o difendersi da un attacco cibernetico.

Si tratta di un interrogativo a cui non è facile dare una risposta esaustiva e questo non soltanto per la relativa novità della materia, ma anche (e soprattutto) perché sono le stesse caratteristiche tipiche dei cyberattacchi a rendere difficile il loro inquadramento nelle tradizionali categorie giuridiche, parametrate su di una concezione (quasi esclusivamente) cinetica di conflitto.

[6] Sul punto, più approfonditamente, si veda: K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New York, 2014.

[7] Per un'analisi più dettagliata degli effetti prodotti dalla *"disclosure"* sul virus *Stuxnet*, si rinvia a: P. Dombrowski, C.C. Demchak, *Rise of a Cybered Westphalian Age*, in *5 Strategic Studies Quarterly* 1, 2011, 32 ss.

[8] Per la teoria della *"difesa in avanti"* (elaborato dal generale P.M. Nakasone, dal 2018 comandante dello *US Cyber Command*) una cyberdifesa realmente efficace non può limitarsi alla semplice protezione dei network nazionali, ma deve "proiettarsi" il più possibile vicino alla sorgente dell'attività ostile, così da: sfruttarne le debolezze, comprenderne le intenzioni e le capacità e (soprattutto) consentire dei contrattacchi decisivi. Per una completa ricostruzione della dottrina in esame si rinvia a *"Achieving and Mantain Cyberspace Superiority. Command vision of US Cyber Command"*, aprile 2018, consultabile all'indirizzo: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf. Invece, per una diffusa critica della nuova dottrina, che sarebbe destabilizzante e servirebbe a mascherare delle vere e proprie operazioni offensive, si rinvia a L. Jinghua, *A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'*, in *Lawfare Blog*, 19 ottobre 2018.

DPCE online
ISSN: 2037-6677

2. Cyberattacchi, definizione e caratteristiche

È pertanto necessario, ai fini del corretto inquadramento del tema trattato e delle problematiche da esso sollevate, affrontare primariamente il problema di carattere definitorio, cercando di capire quale sia la natura e la portata dei cyberattacchi. Per attacco cibernetico[9], stando al glossario pubblicato nel 2011 (in concomitanza all'istituzione dello *US Cyber Command*) dallo Stato maggiore congiunto statunitense, si deve intendere: un'azione ostile posta in essere attraverso un computer o una rete di computer al fine di degradare, disarticolare, distruggere, o impedire l'accesso a computer e reti, ovvero alle informazioni ivi contenute[10]. Tale originaria definizione, pur andando incontro a delle modifiche di natura prettamente stilistica, ha mantenuto (a riprova della sua validità) inalterate le sue caratteristiche di fondo, tant'è che nell'ultima edizione del *"Dictionary of military and associated terms"*, del Dipartimento della Difesa degli Stati Uniti d'America, i *"cyberspace attacks"* vengono identificati come: "actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."[11]
Dunque, le reti di computer e le informazioni in esse immagazzinate, trattandosi di algoritmi codificati volti a diffondere effetti pregiudizievoli in un sistema bersaglio, rappresentano, al contempo, sia l'arma sia l'oggetto dell'attacco informatico.

[9] A fini di maggiore chiarezza, si precisa come dalla nozione di cyberattacco qui fornita (conformemente alla letteratura scientifica in materia) siano escluse tutte quelle attività ostili che integrano la categoria della *"cyberexploitation"*. In estrema sintesi, quest'ultima verrebbe a ricomprendere tutte quelle operazioni dirette, per un periodo di tempo più o meno prolungato, a monitorare ed ottenere le informazioni che risiedono o transitano su di un computer o una rete di computer e che sarebbero altrimenti riservate. La *"cyberexploitation"*, pertanto, si differenzia da un cyberattacco in quanto ha una natura *"non distruttiva"*, non determinando la compromissione o comunque la manipolazione delle informazioni oggetto dell'attività. Resta il fatto che, al di fuori dell'ambito più strettamente scientifico, i due termini continuano ad essere utilizzati come sinonimi e ciò non senza delle ragioni di fondo. In primo luogo, infatti, i cyberattacchi e la *"cyberexploitation"* si distinguono solo in termini di risultati prodotti, ma da un punto di vista puramente tecnico sono molto simili. Secondariamente è molto frequente che queste due tipologie di operazioni siano realizzate congiuntamente (magari dallo stesso programma), nel senso che un cyberattacco può essere propedeutico ad una *"cyberexploitation"* e viceversa. Per i rapporti tra la nozione di cyberattacco e quella di *"cyberexploitation"*, si rinvia a H.S. Lin, *Offensive Cyber Operations and the Use of Force*, in *Journal of National Security Law & Policy* 63, 2010, 63 ss. e A. Wortham, *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?*, in 64 *Federal Communications Law Journal* 3, 2012, 644 ss.

[10] Si veda sul punto: Gen. J.E. Cartwright, *Memorandum for Chiefs of the Military Services, Commander of the Combatant Commands, Director of the Joint Staff Directorates, on Joint Terminology for Cyberspace Operations*, 2011, a sua volta ripreso da: O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, *The Law of Cyber-Attack*, in 100 *California Law Review* 4, 2012, 824.

[11] Sul punto si veda: *Dictionary of military and associated terms, United States Departement of Defense*, 2021, 55.

Tale caratteristica, oltre a distinguerli da ogni altro tipo di attacco "convenzionale", ci permette di evidenziare alcune peculiarità che, nonostante la loro eterogeneità, accomunano ogni forma di cyberattacco[12]. Anzitutto gli attacchi informatici (benché ciò non possa escludersi a livello puramente teorico) non producono direttamente un danno, piuttosto si limitano a manipolare un sistema informatico così da creare una reazione a catena che porti all'evento dannoso desiderato.

In secondo luogo, questa tipologia di attacchi non appartiene al mondo fisico, nel senso che: sia i loro obiettivi (ossia le informazioni contenute all'interno di un sistema informatico), sia i danni da essi prodotti (che consistono nella distruzione o corruzione delle suddette informazioni), sia l'arma da essi utilizzata (il codice binario in cui consistono) esistono ed interagiscono tra loro esclusivamente all'interno del cyberspazio, manifestandosi solo di riflesso nella realtà circostante.

Terza caratteristica dei cyberattacchi è data dall'impossibilità di determinare *ex ante* il loro risultato, in quanto un attacco cibernetico potrebbe non provocare (neppure in via indiretta) un danno, ma limitarsi a degradare o rendere impossibile l'accesso ad un servizio o ad una funzione.

Emblematici al riguardo sono i cosiddetti attacchi DDOS [acronimo di *Distributed Denial Of Services*] che non producono danni, ma si limitano a inondare un sito web o un server di false richieste di accesso (a loro volta prodotte ed inviate da appositi programmi, detti BOTNET) obbligandolo a gestirle e rendendolo inaccessibile agli utenti legittimi[13].

Tali attacchi, molto semplici e molto diffusi[14], possono essere usati per interrompere o bloccare operazioni e sistemi critici sia civili sia militari, come dimostrano i diversi attacchi DDOS lanciati (il 24 febbraio scorso) dal collettivo *Anonymous* contro la Federazione russa e che hanno portato allo *shutdown* di numerosi siti internet di informazione e governativi, tra cui quelli della Duma e del Cremlino.

Infine, i cyberattacchi si caratterizzano per essere difficilmente rintracciabili, nel senso che (anche alla luce degli sviluppi tecnologici) possono essere "instradati" in diversi server sparsi per il mondo prima di raggiungere il loro bersaglio, occultando sia l'identità dell'aggressore sia il luogo fisico da cui è partito l'attacco.

Chiarite la nozione e le caratteristiche dei cyberattacchi, non resta che vedere come il diritto abbia reagito, a livello nazionale ed internazionale, alla comparsa di questi nuovi strumenti bellici.

[12] Sul punto, più nel dettaglio, si rinvia a S. Setti, *Diritto e guerra cibernetica*, 2017, 4 ss e H. Dinnis, *Cyberwarfare and the laws of war*, New York, 2014.

[13] Per un'analisi più approfondita degli attacchi DDOS si rinvia a O.A. Hathaway, R. Crootof, P. Levitz, H.Nix, A. Nowlan, W. Perdue, J. Spiegel, *The Law of Cyber-Attack*, in 100 *California Law Review* 4, cit., 837 ss.

[14] Sul punto, più approfonditamente, si rinvia a E. Tikk, K. Kaska, L. Vihul, *International cyber incidents: legal consideration*, in *NATO CCDCOE*, 2010, 112 ss.

DPCE online
ISSN: 2037-6677

3. Il regime giuridico statunitense

Nonostante ormai quasi tutti gli ordinamenti dedichino alla *cyberwar* specifici regimi giuridici ed apparati[15], in questa sede (vista anche la limitatezza del contributo) pare opportuno focalizzarci sul *"legal framework"* elaborato dagli Stati Uniti d'America e questo non soltanto perché essi continuano a detenere il primato strategico a livello globale nel cyberspazio[16]. Infatti, il regime giuridico che si è sviluppato nel corso degli ultimi anni risulta essere abbastanza articolato[17], pur presentando non poche criticità.

A ben vedere, la ragione di fondo che sta alla base dello sviluppo di questa disciplina (meno conosciuta di quella prevista per le operazioni militari tradizionali, ma non meno importante[18]) e della sua ampiezza può essere identificata nell'annoso contrasto tra il potere esecutivo ed il Congresso in merito alla *"constitutional division"* dei cosiddetti *"war powers"*, con il tentativo di quest'ultimo di creare un sistema normativo che gli garantisca un certo grado di "controllo preventivo" sulle operazioni militari cibernetiche autorizzate dal Presidente.

3.1 I cyberattacchi tra l'assetto costituzionale dei poteri di guerra e la War Powers Resolution

Anzitutto, si osserva come il problema della separazione dei poteri si complichi notevolmente[19] quando viene applicato al tema dei *"war powers"* e questo per la forte incertezza che caratterizza, sul punto, la costituzione statunitense, dal cui testo risulta impossibile ricavare delle indicazioni precise[20]. Nel tentativo di ricostruire l'originaria volontà dei costituenti, si è

[15] Sul punto, a titolo puramente esemplificativo, si rinvia (per una più approfondita ricostruzione del quadro esistente, oltre che negli Stati Uniti d'America, anche: nel Regno Unito, in Francia, Germania e Spagna) a: A. Marrone, E. Sabatino, *Cyber Defence in NATO Countries: Comparing Models*, in *Istituto Affari Internazionali (IAI)*, 5 febbraio 2021.

[16] L'egemonia statunitense nel cyberspazio, sebbene sempre più contesa, deriva sia dall'enorme disponibilità di "infrastrutture della rete" (come: server, cavi, centri di stoccaggio dati etc.) che ne incrementa vertiginosamente il relativo potenziale di attacco e di intercettazione, sia dal fatto che sul loro territorio hanno sede le principali aziende tecnologiche di portata planetaria.

[17] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, New York, 2022, 67 ss.

[18] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 67.

[19] Sul punto si veda: A.P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperation*, in 111 *Michigan Law Review* 3, 2012, 439; J.D. Mortenson, *Executive Power and the Discipline of History*, in 78 *University of Chicago Law Review* 1, 2011, 377 ss.

[20] Al riguardo, si ricorda come la costituzione statunitense qualifichi espressamente il Presidente come *"Commander in Chief of the military"* (art. 2, sezione 2) senza fornire alcuna spiegazione su quale sia il significato di questo titolo e, soprattutto, senza chiarire se esso sia meramente onorifico, o comporti anche l'attribuzione di qualche potere di natura sostanziale. Al contempo, il testo costituzionale (art. 1, sezione 8)

giunti alla conclusione (basandosi sul fatto che non volessero negare al Presidente il potere di rispondere ad un attacco, ma neppure volessero concedergli una facoltà generalizzata di dare inizio alle ostilità[21]) che l'impianto da essi concepito per i *"war powers"* presupponesse la condivisione degli stessi tra Presidente e Congresso, come dimostra il fatto che l'autorizzazione congressuale sia necessariamente richiesta per iniziare una guerra.

Proprio sul termine *"war"* (definita come: "a constitutional terms of art turning on a variety of factors"[22]) si è concentrato, in tempi abbastanza recenti, lo sforzo dell'*Office of Legal Counsel* (da qui OLC) diretto ad elaborare uno schema teorico che permettesse di capire quando la decisione di intraprendere un'operazione militare rendesse necessaria una *"separation of power analysis"* e potesse, dunque, porre il problema della previa autorizzazione congressuale.

Stando all'OLC perché possa sorgere una questione sulla separazione dei poteri è necessario che l'attività militare presa in considerazione abbia raggiunto il livello di "guerra" e pertanto presenti tutta una serie di specifiche caratteristiche, tra le quali si ricorda: "l'exposure of US military personnel to a significant risk over a substantial period"[23].

Appare chiaro come i cyberattacchi e più in generale tutte le *"cyberoperations"* (specie se considerate singolarmente) non riescano, alla luce delle loro caratteristiche tipiche, ad integrare tale standard e pertanto potranno essere sempre decise dal Presidente senza la previa autorizzazione del Congresso.

Ad un risultato analogo si giunge provando a ricondurre gli attacchi informatici nell'alveo della *"War Powers Resolution"* (da qui WPR) e degli obblighi informativi da essa imposti al Presidente per tutte le attività militari intraprese in assenza di una formale dichiarazione di guerra.

Stante la rigida interpretazione (affermatasi sotto l'amministrazione Obama[24]) del concetto di "ostilità", che viene ad includere fattori come il

attribuisce al Congresso importanti prerogative in ambito bellico, tra le quali spiccano: il potere di dichiarare guerra, il compito di provvedere alla difesa comune, la possibilità di stabilire norme per il governo delle forze armate e la facoltà di ordinare la mobilitazione dell'esercito e della marina. Sul punto, per ciò che concerne la definizione del ruolo di *"Commander in Chief"*, si rinvia a D.J. Barron, M.S. Lederman, *The Commander in Chief at the Lowest Ebb-Framing the Problem, Doctrine, and Original Understanding*, 121 *Harvard Law Review* 689, 2008, 767 ss; D.G. Adler, *The Law: George Bush as Commander in Chief: Toward the Nether World of Constitutionalism*, in 36 *Presidential Studie Quarterly* 3, 2006, 525 ss.

[21] Sul punto si rinvia a A.M. Schlesinger Jr, *The Imperial Presidency*, Boston, 1973, 4 ss.

[22] Si veda: R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 72.

[23] Si veda: S.A. Engel, *April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities. Memorandum Opinion for the Counsel to the President*, 2018, 9.

[24] Il riferimento è alla dichiarazione resa da Harold Koh, in qualità di *"State Department legal adviser"*, durante l'audizione indetta (nel 2011) dal *"Foreign Relations Committee"* del Senato sulle implicazioni derivanti dal coinvolgimento statunitense nel conflitto libico. Stando alla risposta fornita da Koh, la nozione di *"hostilities"* non poteva ritenersi integrata in quanto: la missione aveva uno scopo limitato; il rischio di perdite americane era inesistente, posto che non si prevedeva un'occupazione del territorio; non sussisteva

DPCE online
ISSN: 2037-6677

fondato rischio di perdite americane, è pressoché impossibile che un cyberattacco rappresenti una *"introduction of US forces in to hostilities"*[25] e legittimi un'applicazione della WPR e delle previsioni in essa contenute (come, ad esempio, l'obbligo per il Presidente di riferire al Congresso sullo stato dell'operazione entro quarantotto ore dall'inizio della stessa).

3.2 Cyberattacchi e "Covert Action Statue", un'opportunità mancata?

Alla luce del quadro tracciato si capisce come mai gli sforzi del Congresso, volti ad introdurre una forma di controllo *ex ante* delle *"cyber military operations"* autorizzate dal Presidente, si siano concentrati sul cosiddetto *"Covert Action Statute"* (da qui CAS), ossia il regime giuridico originariamente elaborato con lo *"Hughes-Ryan Emendament"* (al *"Foreign Assistance Act)* del 1974.

In tale circostanza, il Congresso, facendo leva sul proprio potere di borsa, rivoluzionò le modalità seguite dal governo per approvare le "operazioni segrete", imponendo che ciascuna di esse fosse preceduta (pena l'impossibilità di utilizzare i fondi appositamente stanziati nel bilancio) da un *"finding"* firmato personalmente dal Presidente[26] ed indicante le caratteristiche dell'operazione e la sua rilevanza per la sicurezza nazionale, da consegnarsi agli *"Intelligence Committees"* di Camera e Senato. L'estensione del regime autorizzatorio previsto dal CAS anche alle *"cyberoperations"*, benché esso fosse stato originariamente concepito per le sole "operazioni segrete" poste in essere dalla CIA, non avrebbe posto particolari problemi, stante l'ampia (e volutamente vaga) nozione di *"covert action"* dallo stesso introdotta e che ricomprendere ogni operazione, posta in essere da qualsiasi apparato del governo statunitense, che sia destinata a produrre un effetto all'estero senza che il coinvolgimento americano sia apparente, o riconosciuto.

Inoltre, ricondurre i cyberattacchi nell'ambito di applicazione del CAS avrebbe determinato indubbi benefici anche per il Presidente, fornendo una maggiore legittimazione costituzionale alle sue scelte in materia.

---

il pericolo di un'escalation; l'impiego di mezzi militari era piuttosto limitato e di certo ben lontano da un *"full military engagement"*. Per una complete ricostruzione delle dichiarazioni di Koh si rinvia a *Separation of Powers — War Powers Resolution — Obama Administration Argues that U.S. Military Action in Libya Does Not Constitute "Hostilities. — Libya and War Powers: Hearing Before the Senate Committee on Foreign Relations, 112th Cong. 7—40 (2011) (statement of Harold Koh, Legal Adviser, U.S. Department of State)"*, in 125 *Harvard Law Review* 6, 2012, 1546 ss.

[25] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 74.

[26] Uno dei principali obiettivi del CAS era proprio quello di eliminare la *"presidential deniability"* in relazione alle *"covert action"*, escludendo in radice la possibilità per il Presidente di sostenere di non essere stato a conoscenza di una determinata operazione. Sul punto, più nel dettaglio, si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 75.

Per comprendere meglio questo profilo è necessario riferirsi brevemente al criterio fornito dal *"Justice"* Jackson nella sua *"concurring opinion"* alla sentenza della Corte Suprema *"Youngstown Sheet & Tube Co. v. Sawyer"*[27] per risolvere le questioni attinenti alla separazione dei poteri tra esecutivo e legislativo[28].

Stando al *"Justice"* Jackson, le azioni presidenziali possono essere suddivise in tre categorie: quelle compiute sulla base di un'autorizzazione (espressa o implicita) del Congresso, per le quali si ha "the strongest presumption of constitutional validity"[29]; quelle intraprese "in the face of congressional silence", dove il rischio di un conflitto con il Congresso fa sì che il Presidente possa fare affidamento sui suoi poteri costituzionali intrinseci[30]; quelle contrarie alla volontà (espressa o implicita) del Congresso, dove i poteri presidenziali sono al loro minimo ed il loro esercizio può considerarsi corretto solo se (date le circostanze) l'autorità costituzionale del Presidente supera quella del Congresso[31]. Come è stato osservato[32], l'applicazione del CAS agli attacchi informatici avrebbe permesso di ricondurre gli atti del Presidente, volti ad autorizzarli, all'interno della prima categoria, garantendogli il supporto del Congresso e ponendolo al riparo dalle possibili conseguenze cui potrebbe andare incontro qualora il cyberattacco producesse degli effetti indesiderati.

Infine, si ricorda come il regime delineato dal CAS, proprio per il fatto di andare a disciplinare delle operazioni che si collocano a metà strada tra l'attività militare e quella di intelligence, presenti un'estrema flessibilità[33],

[27] Si veda: U.S. Supreme Court, *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), 634 ss. (Jackson, J., concurring).

[28] Criterio che, dalla sentenza *Dames & Moore v. Regan*, del 1981, è stato ufficialmente adottato dalla stessa Corte Suprema come *"framework"* per risolvere le controversie in materia di separazione dei poteri. Si veda: U.S. Supreme Court, *Dames & Moore v. Regan*, 453 U.S. 654 (1981), 668 ss.

[29] In particolar modo, questa presunzione di validità costituzionale deriverebbe dal fatto che: *"When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. In these circumstances, and in these only, may he be said (for what it may be worth) to personify the federal sovereignty"*. Sul punto si rinvia a U.S. Supreme Court, *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), 635 e 636 (Jackson, J., concurring).

[30] Si veda: U.S. Supreme Court, *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), 637 (Jackson, J., concurring), ove si osserva: *"When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is Uncertain"*.

[31] In tali casi, tuttavia, lo scrutinio operato dalla Corte Suprema dovrà essere particolarmente attento, infatti: *"Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system"*. Si rinvia a U.S. Supreme Court, *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), 638 (Jackson, J., concurring).

[32] Si veda: A.P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperation*, in 111 *Michigan Law Review* 3, cit., 442 ss.

[33] A riprova di ciò si ricorda come anche all'operazione diretta ad eliminare Osama Bin Laden si sia applicato il CAS e questo nonostante che (dopo la sua riuscita) non si sia fatto nulla per nascondere il coinvolgimento statunitense. Tuttavia, in caso di fallimento dell'operazione il regime giuridico delle *"covert action"* avrebbe fornito

DPCE online
ISSN: 2037-6677

che lo avrebbe reso ideale per disciplinare la vasta gamma delle *"cyber military operation"* ed avrebbe consentito di avere un unico *"legal framework"* utilizzabile da tutte le agenzie[34].

Tuttavia, la volontà di escludere ogni forma di controllo preventivo da parte del Congresso ha portato, anche in questo caso, a negare la riconducibilità dei cyberattacchi alla disciplina del CAS e ciò nonostante i numerosi vantaggi che ne sarebbero derivati.

Per raggiungere tale obiettivo si è fatto leva sulla cosiddetta *"TMA exception"*, contenuta nello stesso CAS, che esclude dalla nozione di *"covert action"* e dagli obblighi di trasparenza ad essa connessi tutte le "traditional military activities or routine support to such activities"[35]. Il problema che si è posto negli ultimi anni, provocando non pochi attriti tra governo e Congresso al momento di autorizzare le *"cyberoperations"*, è stato proprio quello di capire cosa potesse intendersi per attività militare tradizionale all'interno del dominio cibernetico[36].

Sul punto si sono scontrate due opposte visioni: la prima, per salvaguardare il ruolo del Congresso, valorizzava il termine *"traditional"* e limitava l'ambito di applicazione della *"TMA exception"* alle sole operazioni cibernetiche che fossero *"sufficiently analogous"* a quelle cinetiche; la seconda, più vicina alla posizione governativa, enfatizzava, invece, il compromesso definitorio cui erano giunti il Congresso e l'amministrazione e ricollegava l'applicazione dell'eccezione al fatto che l'operazione fosse stata interamente comandata ed attuata dai *"services members"* e condotta in contesti di aperta ostilità, o la cui pianificazione fosse stata approvata dalla *"National Command Authority"*[37].

A risolvere la questione, dopo un primo e fallimentare tentativo di cercare una soluzione di compromesso[38], è stato lo stesso Congresso che,

maggiori garanzie. Sul punto si rinvia a R. Chesney, *On the Legality of Killing UBL Even If He Was Unarmed (and On the Title 50 Issue)*, in *Lawfare blog*, 4 maggio 2011.

[34] Si veda: A.P. Brecher, *"Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperation"*, in 111 *Michigan Law Review* 3, cit., 434 ss.

[35] Sul punto, più nel dettaglio, si rinvia a A.P. Brecher, *"Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperation"*, in 111 *Michigan Law Review* 3, cit. e R. Chesney, *"The Domestic Legal Framework for US Military Cyber Operations"*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit.

[36] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 76, ove si osserva come: *"In recent years, such issues have proved to be a significant source of friction in the approval of military operations in the cyber domain"*.

[37] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit., 77.

[38] Il riferimento è alla sezione 944 del *"National Defense Authorization Act"* per l'anno fiscale 2012, dove il Congresso aveva previsto che: le operazioni militari offensive poste in essere nel cyberspazio fossero soggette al regime giuridico previsto per le operazioni cinetiche, incluso il diritto dei conflitti armati. È evidente come la soluzione di compromesso perseguita dal Congresso mirasse a confermare l'applicabilità della *"TMA exception"* per le sole operazioni cibernetiche offensive, escludendola di converso

nella sezione 1632 del *"National Defense Authorization Act"* per l'anno fiscale 2019, ha rinunciato ad ogni sua prerogativa in materia, stabilendo come: ogni attività o operazione militare "clandestina" posta in essere nel cyberspazio si qualifichi necessariamente come una *"traditional military activity"*[39] e pertanto rientri nella *"TMA exception"*.

Per fugare ogni eventuale dubbio connesso alla natura delle operazioni militari cibernetiche in questione, il Congresso ha anche chiarito[40] come il termine *"clandestine"* ricomprenda: sia la nozione di *"secrecy"* (nel senso che l'operazione viene progettata per non essere scoperta), sia quella di *"deniability"* (ossia che il coinvolgimento del governo nell'operazione non dovrà essere apparente o riconosciuto)[41].

La scelta di ricondurre tutte le *"cyber military operations"* all'interno della *"TMA exception"* lascia perplessi e questo principalmente perché esclude in radice ogni forma di coinvolgimento del Congresso nel processo di progettazione ed autorizzazione di operazioni potenzialmente ad alto rischio per la sicurezza nazionale[42].

Infatti, riprendendo il criterio elaborato dal *"Justice"* Jackson, la mancanza di una previa autorizzazione congressuale finisce inevitabilmente per relegare l'attività del Presidente in materia nella seconda o nella terza categoria[43], esponendolo al rischio di serie ripercussioni qualora un'operazione cibernetica da lui autorizzata integri (anche alla luce del diritto internazionale) *ex post* un uso della forza[44].

In conclusione, lo sviluppo del *"legal framework"* statunitense mostra come il governo abbia utilizzato strumentalmente le incertezze che caratterizzano la nozione di cyberattacco per spogliare, anche in questo settore, il Congresso delle sue prerogative in materia di *"war powers"*, delineando un fragile equilibrio di cui solo il tempo potrà confermarci la riuscita.

per quelle difensive. Tuttavia, è stata proprio l'impossibilità di distinguere tra operazioni militari cibernetiche offensive e difensive a determinare il definitivo fallimento di tale soluzione.

[39] Sul punto si rinvia a R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment*, cit.

[40] Sempre nella sezione 1632 del *"National Defense Authorization Act"* per l'anno fiscale 2012.

[41] Sul punto si veda: R. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, in J. Goldsmith (Ed.), *"The United States Defend Forward Cyber Strategy. A Comprehensive Legal Assessment"*, cit., 79.

[42] I cyberattacchi sono ormai interamente sottoposti al cosiddetto *"Military Regime"*, in cui non si prevede alcun obbligo di notificazione al Congresso, né tantomeno alcuna forma di *"presidential finding"*. Tuttavia, nella medesima sezione 1632 del *"National Defense Authorization Act, for fiscal year 2019"*, il Congresso ha introdotto una nuova regola procedurale che subordina la realizzazione delle *"cyber operations"* all'espressa autorizzazione del Presidente, o (in sua vece) del Segretario alla Difesa.

[43] Sul punto, più in dettaglio, si veda: A.P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperation*, in 111 *Michigan Law Review* 3, cit., 442 ss.

[44] Eventualità quest'ultima che, tenendo a mente le caratteristiche tipiche dei cyberattacchi, non pare poi così remota.

DPCE online
ISSN: 2037-6677

4. Rimedi sul piano del diritto internazionale

Non resta che valutare quali siano i rimedi offerti dal diritto internazionale rispetto a questa nuova tipologia di conflitto.

La prima difficoltà che incontriamo sta proprio nel fatto che i principali trattati internazionali in materia (a partire dalla Carta delle Nazioni Unite e dal Patto Atlantico) delineano un sistema in cui l'inquadramento delle operazioni militari cibernetiche risulta complesso, proprio perché al momento della loro stesura l'informatica non era assolutamente in grado di incarnare una minaccia.

4.1 Cyberattacchi e legittima difesa

Altro problema da porsi è se un attacco cibernetico possa rappresentare un uso della forza armata, ai sensi dell'art. 2, par. 4, della Carta ONU e pertanto possa consentire allo Stato colpito di rispondere invocando il diritto alla legittima difesa individuale e collettiva (art. 51).

Al riguardo, la dottrina maggioritaria ritiene che un cyberattacco possa integrare la nozione di uso della forza, ai sensi dell'art.2, par. 4, solo ed esclusivamente quando produca gli stessi effetti di un attacco convenzionale (cinetico) e dunque sia la causa di un danno fisico (diretto, o indiretto) a cose e/o presone[45].

Per buona parte degli autori[46] la rilevanza degli effetti è tale da sottolineare come il vero problema non sia tanto quello di accertare se un attacco cibernetico integri un uso della forza, quanto piuttosto se a configurarlo sia lo specifico effetto da esso prodotto. In altri termini, secondo questa impostazione teorica, è soltanto l'effetto generato da un attacco informatico (e non il meccanismo utilizzato per provocarlo) a rappresentare l'adeguata base di partenza per una simile analisi. Come si vede, tale interpretazione finisce per escludere dal novero degli attacchi cibernetici cui è lecito rispondere, tutte quelle operazioni di *cyberwarfare* che hanno come obiettivo di aggredire le informazioni contenute in un sistema informatico e che pertanto, pur potendo avere delle conseguenze rilevanti, non producono alcun tipo di danno fisico.

[45] Si vedano ex multis: H. Dinnis, *Cyberwarfare and the laws of war*, cit., 174; M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in 37 *Columbia Journal of Transnational Law* 885, cit. e *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"*, 2017 ; H.H. Koh, *International Law in Cyberspace*, in 54 *Harvard International Law Journal* 13, 2012, 4 ss.; F. Tasdemir, G. Albayrak, *The Law of Cyber Warfare in Terms of Jus Ad Bellum and Jus in Bello: Application of International Law to the Unknown?*, 2017, 6 ss.; H.S. Lin, *Offensive Cyber Operations and the Use of Force*, in 4 *Journal of National Security Law & Policy* 63, cit., 74.

[46] Sul punto, *ex multis*, si rinvia a H.S. Lin, *Offensive Cyber Operations and the Use of Force*, in 4 *Journal of National Security Law & Policy* 63, cit.; M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in 37 *Columbia Journal of Transnational Law* 885, 1998; J. Barkham, *Information Warfare and International Law on the Use of Force*, in 34 *New York University Journal of International Law and Politics* 57, 2001, 84 ss.

Non mancano opinioni dissenzienti[47]che, ricordando come la società moderna sia estremamente vulnerabile anche a questa tipologia di attacchi informatici, legittimano anche in questi casi la possibile risposta armata dello Stato aggredito.

Si tratta, tuttavia, di un'interpretazione da molti valutata come troppo *estensiva*, in quanto consentirebbe di ricorrere alla forza armata anche in assenza del necessario presupposto del danno di natura fisica.

Secondo Marco Roscini, invece, per capire se un cyberattacco integri o meno la nozione di uso della forza è necessario guardare al suo bersaglio, piuttosto che agli effetti da esso prodotti. In altri termini, seguendo questo *"target oriented approach"*, ad uno Stato sarebbe consentita la reazione in legittima difesa tutte le volte in cui un attacco informatico colpisca le sue infrastrutture critiche (come, ad esempio, le reti di distribuzione dell'energia elettrica) e questo a prescindere dal fatto che lo stesso infligga dei danni fisici[48].

Tuttavia, anche questo approccio non è condiviso dalla dottrina maggioritaria e questo non soltanto perché esso legittimerebbe, senza alcuna valutazione sul rispetto del criterio di *proporzionalità*, la risposta armata dello Stato anche a fronte di un attacco a bassissima intensità, purché diretto alle infrastrutture critiche.

Infatti, come riconosce lo stesso Roscini[49], a sollevare numerosi problemi è anche l'incertezza connaturata alla nozione di *"critical infrastructures"* e, soprattutto, se nella stessa possano essere ricompresi anche i network delle grandi infrastrutture civili che, pur non appartenendo allo Stato, risultano essenziali per la collettività. Così, riprendendo l'esempio già formulato dallo stesso Autore, non è chiaro se una *"cyber military operation"* diretta contro *Google* possa integrare, visto il ruolo egemone assunto dall'azienda californiana, un attacco alle infrastrutture critiche statunitensi e, pertanto, permettere una loro risposta in legittima difesa[50].

Degna di nota è anche la tesi proposta da Russel Buchan[51] e che, in aperta controtendenza rispetto alla prevalente letteratura in materia, individua nel *"principio di non intervento"* lo strumento più idoneo a tutelare gli Stati dai cyberattacchi privi di conseguenze sul piano fisico.

Secondo l'Autore, infatti, il principio in questione, sancito dal diritto internazionale consuetudinario, verrebbe a delineare: "a legal framework

[47] Sul punto si veda: W.G. Sharp, *Cyberspace and the use of force*, Falls Church, 1999, 129 ss; G. Kerschischnig, *Cyberthreats and International Law*, 2012; S. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, 2014, 289 ss.

[48] Per ulteriori approfondimenti sul *"target oriented approach"*, si rinvia a M. Roscini, *World Wide Warfare* - Jus ad bellum *and the Use of Cyber Force*, in 14 *Max Planck Yearbook of United Nations Law* 85, 2010, e *Cyber Operations and the Use of Force in International Law*, Oxford, 2014.

[49] Sul punto, più nel dettaglio, si veda: M. Roscini, *World Wide Warfare* - Jus ad bellum *and the Use of Cyber Force*, in 14 *Max Planck Yearbook of United Nations Law* 85, cit., 117 ss.

[50] L'esempio è ripreso da: M. Roscini, *World Wide Warfare* - Jus ad bellum *and the Use of Cyber Force*, in 14 *Max Planck Yearbook of United Nations Law* 85, cit., 117.

[51] Sul punto, si rinvia a R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in 17 *Journal of Conflict & Security Law* 2, 2012, 217 ss.

DPCE online
ISSN: 2037-6677

that can protect States from cyber attacks which, although not producing physical damage and thus not qualifying as an unlawful use of force, nevertheless have the effect of coercing a State into adopting a course of conduct that it is freely entitled to determine itself"[52].

Comunque, anche ammettendo la possibilità di rispondere in legittima difesa ad un attacco cibernetico, resta da risolvere il problema dell'imputabilità dello stesso, al fine di capire verso chi indirizzare l'eventuale risposta.

L'incertezza, che caratterizza sotto questo profilo la guerra cibernetica, non solo rende molto difficile individuare l'autore ed il mandante (pare improbabile che uno Stato rivendichi espressamente una siffatta operazione, come dimostra l'atteggiamento tenuto dal governo nordcoreano a seguito del sabotaggio del sistema informatico della *Sony Corporation*[53]) di un cyberattacco, ma aumenta notevolmente il rischio di attribuire erroneamente l'attacco ad un paese terzo.

Ci limitiamo a ricordare come allo stato attuale manchino riferimenti normativi e giurisprudenziali sufficienti a risolvere il problema e che l'unico appiglio in materia sia la regola generale per cui: ogni stato che contribuisca materialmente o moralmente, ad un attacco possa essere destinatario della reazione in legittima difesa, purché la vittima dell'attacco riesca a provarne la partecipazione[54].

In ogni caso, l'eventuale reazione in legittima difesa dovrà rispettare i requisiti della *necessità*, nel senso che l'esigenza dell'uso della forza deve essere urgente ed irresistibile, e della *proporzionalità*, che deve essere parametrata all'obiettivo della risposta e non al mezzo impiegato e che pertanto legittima una reazione *"cinetica"* ad un attacco cibernetico[55].

Ad oggi, l'unico caso "noto" di reazione convenzionale ad un attacco informatico si è realizzato nel 2019, quando lo Stato di Israele, vittima di un cyberattacco da parte di Hamas, ha deciso di distruggere il quartier generale informatico dell'organizzazione mediante il lancio di missili[56].

---

[52] Si veda: R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in 17 *Journal of Conflict & Security Law* 2, cit., 226.

[53] Nonostante l'FBI, la NSA e lo stesso Presidente Obama avessero indicato la Corea del Nord come "mandante" dell'attacco cibernetico condotto ai danni della casa di produzione cinematografica, il governo nordcoreano ha ripetutamente negato il proprio coinvolgimento ed ha chiesto un'inchiesta congiunta sull'accaduto, per maggiori informazioni si rinvia a *"North Korea demands joint inquiry with US into Sony Pictures hack"*, in *The Guardian*, 20 dicembre 2014, consultabile all'indirizzo: https://www.theguardian.com/world/2014/dec/20/north-korea-proposes-joint-inquiry-us-sony-pictures-hack; S. Setti, *Diritto e guerra cibernetica*, cit.

[54] Diversamente non manca una copiosa letteratura di matrice internazionalistica in materia; tuttavia, considerata la vastità delle opere dedicate al tema, in questa sede ci limitiamo (per consentire un maggiore approfondimento ed il reperimento di ulteriori riferimenti bibliografici) a rinviare *ex multis* alla più recente monografia in lingua italiana dedicata all'argomento, ovvero a: A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli (ESI), 2023.

[55] Sul punto si veda: S. Setti, *Diritto e guerra cibernetica*, cit.

[56] Si veda: *"I missili in risposta a un attacco cyber: così Israele riscrive la cyberwar"*, in *Agenda Digitale*, 10 maggio 2019, consultabile all'indirizzo: https://www.agendadigitale.eu/sicurezza/i-missili-in-risposta-a-un-attacco-cyber-cosi-israele-riscrive-la-cyber-war/

5. Gli sviluppi per il futuro, tra nuove minacce e possibili risposte

Nel mentre, la *Cyberwar* continua ad evolversi e ad ampliare il suo ambito operativo, tanto che in molti hanno definito la guerra Russo-Ucraina una "prima assoluta", proprio per il grande numero di operazioni militari che si stanno conducendo nel cyberspazio e per il fatto di essere incessantemente documentata sui social media[57].

La Russia, nei giorni immediatamente precedenti l'inizio delle ostilità, ha lanciato una *"cyber campaing"* su vasta scala contro l'Ucraina ed al cui culmine (raggiunto il 23 febbraio 2022, alla vigilia dell'assalto armato) si è avuto il più grande attacco DDOS mai registrato nella storia[58]. Il cyberattacco ha messo *offline* più di 600 siti web strategici (tra cui quelli del Ministero degli Esteri e del Ministero della Difesa), bloccando le attività delle principali banche nazionali e causando notevoli problemi alle infrastrutture elettriche e ferroviarie, oltre a determinare l'invio di SMS fraudolenti diretti a fomentare il panico nella popolazione. Ma, già agli inizi di gennaio il *ransomware* denominato *"WhisperGate"* aveva colpito i network di più di 70 organizzazioni pubbliche e private ucraine, probabilmente allo scopo di sottrare dati ed informazioni essenziali al lancio dell'operazione militare[59].

Le *"cyber military operations"* della Russia non si sono, comunque, limitate alle sole fasi inziali del conflitto, come dimostra l'attacco informatico che (il 3 marzo 2022) ha disabilitato la rete elettrica della città di Sumy, nel nord-est ucraino, poco prima che i carri armati russi raggiungessero l'abitato[60]. Analogamente, gli attacchi missilistici contro Dnipro sono stati preceduti da una serie di *"destructive cyberattacks"* che hanno messo fuori uso i siti dei principali enti governativi della città[61] ed è stata appurata (sebbene restino ancora incerte le loro finalità) la presenza di *hacker* ostili nei network di *Energoatom* prima dell'occupazione militare della centrale nucleare di Zaporizhzhya[62].

Gli attacchi informatici russi, oltre a denotare un elevatissimo grado di coordinamento tattico tra le operazioni militari cibernetiche e quelle cinetiche, si caratterizzano anche per la partecipazione su vasta scala di attori non statali, dimostrando come gli sviluppi tecnologici abbiano posto fine al monopolio degli Stati sulle *"cyber offensive capabilities"* ed abbiano

[57] Si veda: C. Morelli, *Cyber war e diritto bellico: le risposte che il diritto internazionale non ha*, *Altalex*, 7 marzo 2022.
[58] Sul punto, più nel dettaglio, si rinvia a P.E. Nilsson, *Unravelling the Myth of Cyberwar. Five Hypoteses on Cyberwarfare in the Russo-Ukrainian War (2014-2023)*, 2023, 44 ss.; J.A. Guerrero-Saade, *"HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine"*, in *SentinelLabs*, 23 febbraio 2022; J. Bateman, *How Militarily Effective Have Russia's Cyber Operations Been in Ukraine?*, in *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, 2022, 5 ss.
[59] Per una ricostruzione più dettagliata degli eventi, si rinvia a C. Strömblad, *State-Sponsored Cyber Attacks Against Ukraine*, in *Trusec*, 19 gennaio 2022.
[60] Sul punto, si rinvia a P.E. Nilsson, *"Unravelling the Myth of Cyberwar. Five Hypoteses on Cyberwarfare in the Russo-Ukrainian War (2014-2023)"*, cit., 41.
[61] Sul punto, si rinvia a *"Defending Ukraine: Early Lessons from the Cyber War"*, Microsoft, 22 giugno 2022, 8.
[62] Al riguardo, più nel dettaglio, si rinvia a P.E. Nilsson, *Unravelling the Myth of Cyberwar. Five Hypoteses on Cyberwarfare in the Russo-Ukrainian War (2014-2023)*, cit.

DPCE online
ISSN: 2037-6677

definitivamente aperto la strada alle *"proxy wars"* anche nello spazio cibernetico[63]. Così, a titolo di esempio, si ricordano i ripetuti attacchi *hacker* che il gruppo *"Armageddon"* ha lanciato, dall'inizio del conflitto, contro le organizzazioni ed i civili ucraini, al fine di saggiare lo stato d'animo del paese e di diffondere *"fake news"* utili allo svolgimento delle operazioni sul campo[64].

Come si vede, le ostilità stanno dimostrando come i cyberattacchi possano prendere di mira non soltanto le infrastrutture (militari e civili) strategiche, ma anche i dati dei singoli utenti privati che, contenuti spesso in *cloud* poco strutturati e curati, rappresentano una preda facile per gli *hacker* ostili.

L'attacco ai dati privati, oltre che per finalità meramente lucrative o di disturbo (si pensi ai cosiddetti *ransomware*) potrebbe avvenire per carpire i segreti industriali del nemico, o (scenario ancora peggiore) per diffondere in modo mirato *deepfake* (magari ricorrendo ai nuovi media sintetici, con cui si potrebbe creare facilmente un finto annuncio di un'autorità governativa, o locale, imitandone anche la voce) così da sobillare crisi e tensioni sociali, o per fornire false informazioni alla popolazione civile in vista di un imminente attacco militare[65].

Si tratta di scenari inquietanti e che dimostrano il crescente potenziale delle armi cibernetiche, ma rispetto ai quali è ancora impossibile trovare un rimedio sul piano giuridico.

Anzi, piuttosto che fornire un'adeguata regolamentazione al fenomeno, le attuali linee di tendenza sembrano dirette a sfruttare le intrinseche ambiguità dei cyberattacchi per escluderne l'inquadramento in un determinato regime giuridico[66].

Lo sviluppo del *"legal framework"* statunitense dimostra come la natura ibrida delle *"cyber military operations"* sia stata utilizzata strumentalmente per sottrarle alle prerogative ed ai controlli del Congresso ed affidarle, in via esclusiva, alla competenza dell'esecutivo.

Così, il carattere *indiretto* degli effetti dei cyberattacchi ha portato a negarne la riconducibilità al concetto di "guerra" costituzionalmente inteso e pertanto anche dall'applicazione di una possibile *"separation of power analysis"*, oltre che alla disciplina contenuta all'interno della WPR.

Le incertezze proprie degli attacchi cibernetici, però, sono state parimenti usate per giustificarne la riconduzione all'interno della cosiddetta *"TMA exception"*, equiparandoli (non senza contraddizioni) alle tradizionali operazioni militari cinetiche ed escludendoli dall'ambito di applicazione del CAS.

Anche sul piano del diritto internazionale, le caratteristiche tipiche dei cyberattacchi continuano ad impedire l'individuazione di una disciplina giuridica idonea a regolamentarli.

---

[63] Sul punto, si veda: S. Duguin, P. Pavlova, *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, 2023, 10 ss.

[64] Sul punto, si rinvia a E. Pinko, *The Cyber Domain in the Russo-Ukrainian War*, in 2 *BESA Center Perspectives Paper*, 2023.

[65] Più nel dettaglio si rinvia a S.R. Soare, J. Burton, *Smart Cities, Cyber Warfare and Social Disorder*, cit.

[66] Sul punto, si rinvia a A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, cit., 261.

La peculiare natura dei loro effetti, destinati a manifestarsi esplicitamente solo nello spazio cibernetico, esclude che la maggior parte di essi integri la nozione di uso della forza e possa pertanto consentire allo stato (eventualmente) aggredito di reagire in legittima difesa.

Al riguardo, riprendendo le considerazioni svolte da Georg Kerschischnig[67], sembra ormai indispensabile procedere ad una profonda ridefinizione dello stesso concetto di *"uso della forza"*, destinata a sancire la definitiva equivalenza tra i *"non-physical damages"* e quelli di natura fisica inflitti dalle tradizionali armi convenzionali. Un cambio di paradigma che, come osserva lo stesso Autore[68], troverebbe la propria legittimazione: sia nella crescente pericolosità dei cyber attacchi, sia nel progressivo riconoscimento dei dati e degli *"intangible assets"* come veri e propri oggetti del diritto di proprietà. In questo modo, anche gli attacchi cibernetici destinati a distruggere le informazioni immagazzinate nella rete, senza produrre alcuna conseguenza effettiva sul piano fisico, potrebbero integrare la nozione di "uso della forza", andando a determinare una *"destruction of property"* e legittimando la risposta dello Stato aggredito.

Tuttavia, anche tale soluzione, per quanto auspicabile, non risulta completamente esaustiva e questo anzitutto perché: essa non fornisce alcuna risposta a tutte le *"cyber military operations"* che hanno come obiettivo la semplice manipolazione dei dati e che, pertanto, non ne determinano la distruzione. Inoltre, resta ferma la forte incertezza che contraddistingue i cyberattacchi e che rende quasi impossibile la corretta individuazione dei loro autori e (soprattutto) dei loro mandanti, con il conseguente rischio di una loro erronea attribuzione.

Pare sempre più necessario che la comunità internazionale, raccogliendo le richieste avanzate da un numero sempre maggiore di stati e di attori non statali (tra cui le principali multinazionali del settore, a partire da Microsoft), prenda in seria considerazione la stesura di un nuovo trattato che permetta di dare una disciplina compiuta ed uniforme al cyberspazio ed alle sue complesse e molteplici articolazioni, ossia quella che da molti viene già chiamata come la *"Digital Geneva Convention"*[69]. Sebbene un nuovo trattato internazionale possa garantire un maggior grado di certezza giuridica, esso (come osserva Stiano[70]) è estremamente difficile da realizzare e non è, comunque, esente da criticità.

Infatti, oltre al forte rischio di non raggiungere un numero sufficiente di ratifiche per la sua entrata in vigore, adottare la forma del trattato farebbe perdere quell'elasticità necessaria a governare una materia in continua evoluzione come quella degli attacchi informatici.

In conclusione, riprendendo le considerazioni svolte dallo stesso Autore, è necessario ricordare il ruolo assolutamente centrale che, in questo

---

[67] Sul punto, più nel dettaglio, si veda: G. Kerschischnig, *Cyberthreats and International Law*, cit., 135 ss.

[68] Si rinvia a G. Kerschischnig, *Cyberthreats and International Law*, cit., 136.

[69] Sul punto si rinvia a: C. Talem, *International law in cyberspace: cyber attacks as use of force*, in *Centro di Studi Strategici, Internazionali e Imprenditoriali*, 2020, 15, consultabile all'indirizzo: https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2020_Talem_Cecilia.pdf.

[70] Sul punto, si rinvia a: A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, cit., 270 ss.

DPCE online
ISSN: 2037-6677

settore, svolgono e continueranno a svolgere i giudici e le prassi interne ai singoli Stati, in quanto in grado di riflettere "quella logica di effettività a cui l'ordinamento internazionale, per sua natura, non ha mai smesso di attingere"[71].

Guido Valenti
Dipartimento di Scienze Giuridiche
Università degli Studi di Pisa
guido.valenti@phd.unipi.it

[71] Sul punto, si veda: A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, cit., 271.