SIOI
UNA Italy
OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

La *Declaration on a common understanding of international law in cyberspace* del Consiglio dell'Unione europea

Pietro Gargiulo
Professore ordinario di Diritto internazionale, Università degli Studi di Teramo; Direttore dell'Osservatorio Osorin

1. *Premessa.* – Il 18 novembre 2024 il Consiglio dell'Unione europea ha adottato la *Declaration on a Common Understanding of International Law in Cyberspace*. Il documento[1] riveste grande importanza sui piani sia politico sia giuridico. Sul piano politico esso mostra, a fronte della recrudescenza del fenomeno degli attacchi cibernetici, che sta diventando estremamente pericoloso specialmente nei tanti conflitti in corso[2], la volontà di affrontare il tema confrontandosi con gli altri interlocutori governativi. Sul piano giuridico la Dichiarazione riafferma l'idea, condivisa dagli Stati membri dell'Unione insieme alla gran parte degli Stati occidentali, che le regole del diritto internazionale così come attualmente in vigore, sono applicabili non solo nel dominio cinetico ma anche in quello cibernetico.

La Dichiarazione parte da una premessa chiara e preoccupante: la minaccia che l'uso malevolo dello spazio cibernetico rappresenta per «the functioning of our societies, economies, and our way of life». Inoltre, il documento evidenzia che tali comportamenti non solo costituiscono un pericolo per le infrastrutture critiche, ma anche un ostacolo sia all'utilizzo dei vantaggi – non solo economici – che derivano dalla digitalizzazione, sia alle iniziative volte a colmare il "digital divide".

Soprattutto, nella premessa della Dichiarazione ciò che si mette in evidenza è la complessità che hanno assunto le attività cibernetiche malevole in concomitanza con l'emergere delle nuove tecnologie dell'informazione e delle comunicazioni (ICT) e l'enorme rilievo delle stesse nei diversi conflitti interni e internazionali che caratterizzano la fase attuale delle relazioni internazionali. Da ciò la necessità che gli Stati agiscano in modo responsabile nello spazio cibernetico, in conformità alla Carta dell'ONU, per garantire il mantenimento della pace, della sicurezza e della stabilità internazionali.

Il richiamo più importante contenuto nella premessa della Dichiarazione – anche perché ci fa capire il contesto materiale nel quale la stessa si inserisce – è quello relativo alla *UN framework of responsible State behaviour in cyberspace* e alla *Cyber programme of action initiative*, entrambi volti a rafforzare la cooperazione internazionale e multi-stakeholder nel settore.

[1] General Secretariat of the Council, *Declaration on a Common Understanding of International Law in Cyberspace*, 15833/24, 18 novembre 2024.

[2] Un significativo esempio è costituito dal conflitto conseguente all'aggressione russa nei confronti dell'Ucraina del febbraio 2022. È noto che la strategia russa è stata caratterizzata da azioni militare precedute o accompagnate da attacchi cibernetici e che anche la risposta militare ucraina ha incluso operazioni cibernetiche condotte con l'aiuto di *teams* militari *cyber* occidentali e da imprese del settore della sicurezza cibernetica. V. P. Gargiulo, *Nazioni Unite*, cybersecurity *e diritto internazionale*, in O. Porchia, M. Vellano (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future.* Liber Amicorum *in onore di Edoardo Greppi*, Napoli-Torino, 2023, 53 ss., spec. 53-54. V. anche M.C. Vitucci, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in *La Comunità Internazionale*, 2023, 7 ss.

Per tale motivo nel prosieguo di questo lavoro incominceremo ad analizzare le due iniziative appena citate, per poi soffermarci sul contenuto della Dichiarazione articolato, nell'annesso alla stessa, in tre pilastri: i diritti e i doveri degli Stati; l'attribuzione delle condotte degli Stati che comportano la responsabilità internazionale; le risposte degli Stati. Non sempre sarà possibile soffermarsi su tutti gli aspetti normativi ai quali si fa riferimento nei pilastri indicati. Tuttavia, è obiettivo di questo lavoro soffermarsi su alcuni di quelli più problematici e al centro delle posizioni divergenti assunte dagli Stati. Nella parte conclusiva verranno svolte alcune considerazioni critiche.

2. *L'*UN framework of responsible State behaviour in cyberspace *e il* Cyber programme of action initiative. – L'uso delle tecnologie digitali sta avendo un impatto notevole in diversi ambiti, ivi compreso quello delle relazioni internazionali. In tale contesto da tempo si è sviluppato un confronto tra gli Stati caratterizzato dai tentativi di acquisire una supremazia tecnologica, premessa indispensabile per conquistare posizioni egemoniche a livello sia internazionale sia regionale. Ciò anche attraverso comportamenti non sempre rispettosi delle regole che reggono l'ordine internazionale.

È per tale motivo che l'ONU, da diverso tempo, si prodiga nel tentativo di favorire l'adozione di un quadro normativo internazionale capace di contrastare l'uso malevolo dello spazio cibernetico. Le iniziative rivolte a tale fine sono riconducibili all'Assemblea generale e alle attività del Gruppo di esperti governativi (GGE) sugli sviluppi nel campo delle tecnologie dell'informazione e delle comunicazioni[3]. In un rapporto del 2013, nella parte relativa alle «raccomandazioni sulle norme, le regole e i principi relativi ai comportamenti responsabili degli Stati»[4], il Gruppo di lavoro in questione sottolineava che l'applicazione delle norme esistenti del diritto internazionale rilevanti per l'uso delle ICT costituiva una misura essenziale per ridurre i rischi per la pace, la sicurezza e la stabilità internazionali. Il rapporto evidenziava la necessità di ulteriori approfondimenti su come tali norme dovessero essere applicate rispetto all'uso delle ICT, ma non mancava di richiamare, specificamente, le regole relative alla sovranità e le norme e i principi che dalla stessa derivano, al rispetto dei diritti e delle libertà fondamentali, alla lotta alla criminalità e al terrorismo, alla responsabilità per comportamenti illeciti.

L'Assemblea generale, dal canto suo, in una risoluzione del 2015 riprendeva le indicazioni del rapporto del GGE 2013 e sottolineava l'importanza sia dell'applicazione del diritto internazionale – in particolare la Carta dell'ONU – quale elemento essenziale per mantenere la pace e la stabilità e promuovere un ambiente ICT aperto, sicuro, stabile, accessibile e pacifico, sia dell'utilizzo volontario di regole e principi non vincolanti relativi a comportamenti responsabili degli Stati per quanto concerne le ICT in quanto potenzialmente idonei a ridurre i rischi per la pace, la sicurezza e la stabilità internazionali[5]. In questa risoluzione si fa riferimento anche al rapporto del GGE 2015[6]

[3] Per indicazioni più ampie, oltre al lavoro citato alla nota precedente si rinvia a P. Gargiulo, *United Nations and Cybersecurity*, in P. Gargiulo, D. Giovannelli, A. L. Sciacovelli (eds.), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspective*, Napoli, 2024, 23 ss.

[4] UN Doc. A/68/98 del 24 giugno 2013, 8-9.

[5] V. la risoluzione 70/237 adottata per *consensus* il 23 dicembre 2015.

[6] UN Doc. A/70/174 del 22 luglio 2015.

suggerendo agli Stati di seguirne le indicazioni per quanto concerne il l'uso delle ICT. In particolare, in detto rapporto vengono raccomandate agli Stati undici regole volontarie e non vincolanti per favorire la promozione di comportamenti responsabili nello spazio cibernetico[7].

Fondate sul diritto internazionale, in particolare sulla Carta dell'ONU, le undici regole che formano il quadro giuridico di riferimento prescrivono, nella gran parte (ben otto), azioni che gli Stati dovrebbero incoraggiare, mentre le altre tre regole riguardano azioni che gli Stati dovrebbero evitare.

Per quanto concerne le prime si fa riferimento: alla cooperazione per sviluppare e applicare misure per rafforzare la stabilità e la sicurezza nell'uso delle ICT e per prevenire l'utilizzo di prassi riconosciute come pericolose o che possono minacciare la pace e la sicurezza; alla necessità, in caso di incidenti determinati dall'uso delle ICT, di considerare tutte le informazioni rilevanti, incluso il contesto più generale dell'evento, le difficoltà dell'attribuzione e la natura e l'estensione delle conseguenze; al rafforzamento della cooperazione per fronteggiare l'uso delle ICT da parte di terroristi e criminali, in particolare attraverso lo scambio di informazioni e l'assistenza reciproca, anche in campo giudiziario; al rispetto dei diritti umani e della *privacy* nell'uso delle ICT in conformità alle risoluzioni del Consiglio dei diritti umani e dell'Assemblea generale[8]; all'adozione di misure appropriate per proteggere le infrastrutture critiche da minacce derivanti dall'uso delle ICT[9]; alla necessità che gli Stati rispondano in maniera adeguata alle richieste di assistenza da parte di altri Stati le cui infrastrutture critiche sono state oggetto di attacchi malevoli; all'adozione di iniziative ragionevoli per garantire l'integrità della catena di fornitura così da promuovere la fiducia nell'utilizzo dei prodotti ICT e per prevenire la proliferazione di strumenti, tecniche e funzioni nascoste dannosi; alla segnalazione di vulnerabilità delle ICT e alla condivisione di eventuali rimedi.

Per quanto concerne le seconde, si fa riferimento al fatto che gli Stati non devono: consapevolmente consentire che il proprio territorio sia utilizzato per commettere illeciti internazionali attraverso le ICT; condurre o consapevolmente appoggiare attività attraverso le ICT che sono contrarie ai loro obblighi internazionali e che intenzionalmente danneggiano infrastrutture critiche o che in altro modo compromettono l'uso e l'operatività di infrastrutture critiche che forniscono servizi pubblici; condurre o consapevolmente appoggiare attività volte a danneggiare le squadre di pronto intervento per gli interventi di emergenza per incidenti in campo informatico o di *cybersecurity*.

È facile intuire che, attraverso queste regole, volutamente ed espressamente indicate come volontarie e non vincolanti, si vuole tentare di rendere più prevedibili i comportamenti degli Stati nello spazio cibernetico e, di conseguenza, rafforzare la sicurezza e promuovere la fiducia nei loro reciproci rapporti in tale ambito. Dal punto di

[7] Ivi, 7-8.

[8] In particolare, questa regola fa riferimento alle risoluzioni del Consiglio dei diritti umani 20/8 e 26/13 sulla promozione, protezione e il godimento dei diritti umani su Internet e alle risoluzioni dell'Assemblea generale 68/167 e 69/166 sul diritto alla *privacy* nell'era digitale.

[9] Anche qui si fa riferimento a una risoluzione dell'Assemblea generale, la 58/199 adottata il 23 dicembre 2003 dedicata a *Creazione di una cultura globale di cybersecurity e la protezione delle infrastrutture critiche dell'informazione*.

vista del contenuto, si suggeriscono comportamenti che appaiono ragionevoli e coerenti con il fine indicato. D'altra parte, il richiamo diffuso agli obblighi che gli Stati hanno ai termini del diritto internazionale e della Carta delle Nazioni Unite giustifica l'utilizzo nei documenti esaminati di espressioni come quadro *giuridico* internazionale o *norme* in riferimento alle regole indicate. Infine, è utile anche sottolineare che il contenuto delle undici regole di cui si è detto è stato ulteriormente specificato nell'ultimo rapporto disponibile del GGE 2019-2021 attraverso l'indicazione di misure che gli Stati potrebbero adottare a livello sia nazionale sia regionale[10].

Per chiudere su questo aspetto, riteniamo utile fare riferimento proprio a una ulteriore iniziativa volta a promuovere l'adozione da parte degli Stati di comportamenti responsabili nello spazio cibernetico. Ci riferiamo alla *Cyber programme of action initiative*, appoggiata da cinquantaquattro Stati e finalizzata a favorire progressi concreti nei comportamenti responsabili degli Stati nello spazio cibernetico tramite misure mirate per: identificare le sfide e promuovere le raccomandazioni e la cooperazione necessarie a farvi fronte; fornire sostegno concreto agli sforzi per il rafforzamento del *capacity-bulding*, anche attraverso uno specifico gruppo di lavoro; promuovere il coinvolgimento significativo di tutti i portatori d'interesse[11].

3. *I contenuti della Dichiarazione del Consiglio dell'UE sull'applicazione del diritto internazionale nello spazio cibernetico: a) aspetti generali*. – Come ricordato in premessa, la Dichiarazione, dopo aver riaffermato, a nome dell'Unione e dei suoi Stati membri, che il diritto internazionale – in particolare la Carta dell'ONU – si applica totalmente nello spazio cibernetico, indica in tre pilastri una lista non esaustiva di elementi giuridici pertinenti al tema.

Qui di seguito daremo indicazione dei pilastri e delle regole giuridiche alle quali si fa riferimento. Successivamente, ci dedicheremo all'esame di alcune delle regole indicate nei pilastri, scelte sulla base del fatto che costituiscono ancora elementi di dibattito e confronto tra gli Stati nella ricerca della definizione del *framework* normativo generale applicabile allo spazio cibernetico. Nell'ambito di questo approfondimento cercheremo di dare indicazione delle posizioni assunte dagli Stati, singolarmente o collettivamente attraverso organizzazioni regionali.

4. *Segue: b) Il primo pilastro della Dichiarazione: i diritti e gli obblighi degli Stati*. – Il primo pilastro relativo ai diritti e agli obblighi degli Stati elenca, anzitutto, la *sovranità statale* come principio fondamentale del diritto internazionale e le regole internazionali che dallo stesso discendono, in base alle quali gli Stati hanno diritto ad esercitare la loro giurisdizione territoriale, tra l'altro, sulle infrastrutture ICT situate sul loro territorio e sulle persone impegnate in attività cibernetiche nel loro territorio. In

[10] V. UN Doc. A/76/135 del 14 luglio 2021, 8-17.

[11] In proposito v. *Working paper for a Programme of Action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security* reperibile online su document.unoda.org. V. anche UN Doc. A/C.1/77/L.73 del 13 ottobre 2022.

campo cibernetico una violazione dell'obbligo di rispettare la sovranità viene individuata rispetto a operazioni attribuibili a uno Stato che violano l'integrità territoriale di un altro Stato o che interferiscono o si impadroniscono di funzioni governative di un altro Stato.

Come corollario della sovranità e dell'uguaglianza sovrana degli Stati viene poi indicato il *principio di non-intervento* che, come è ampiamente noto, costituisce una consolidata regola di diritto internazionale consuetudinario che pone il divieto di intervenire direttamente o indirettamente negli affari di un altro Stato. La sua applicazione in campo cibernetico fa sì che interferenze da parte di uno Stato con i sistemi ICT, i servizi *cloud* e i *networks* nel territorio o sotto la giurisdizione di un altro Stato senza il suo consenso possono costituire un intervento proibito ai termini del principio in questione.

Anche la *due diligence* – l'obbligo degli Stati di non consentire che il loro territorio sia usato per atti contrari ai diritti di un altro Stato – è un principio di diritto internazionale ritenuto applicabile nel contesto *cyber*. In particolare, ai termini di tale principio gli Stati devono fare tutto ciò che è nelle loro possibilità affinché le loro infrastrutture ICT non siano usate da attori statali e non statali per atti o attività che violano i diritti di altri Stati. Inoltre, agli Stati è fatto obbligo di adottare tutte le misure appropriate, ragionevoli e praticabili per agire contro operazioni cibernetiche che violano i diritti di altri Stati.

Molto importante in questo primo pilastro della Dichiarazione è il riferimento al *divieto dell'uso della forza*. Si tratta di un aspetto la cui applicazione alla dimensione cibernetica sta sollevando particolari difficoltà nel negoziato volto alla definizione del *framework* internazionale applicabile. Per tale motivo lo analizzeremo a parte successivamente.

Nel primo pilastro la Dichiarazione fa anche riferimento al *rispetto del diritto internazionale umanitario* (DIU). Anche questo è un aspetto oggetto di difficoltà nell'ambito del negoziato internazionale. La Dichiarazione, sul punto, afferma che il DIU si applica alle operazioni cibernetiche nell'ambito dei conflitti sia internazionali sia interni. In particolare, nella Dichiarazione si fa riferimento ai principi fondamentali del DIU – umanità, necessità militare, distinzione, proporzionalità –, nonché al rispetto degli obblighi che disciplinano la condotta delle ostilità. Inoltre, una particolare enfasi è posta sul rispetto del principio di distinzione, che impone alle parti del conflitto di dirigere i loro attacchi militari esclusivamente contro obiettivi militari e combattenti, anche se si tiene conto della difficoltà di applicazione al dominio cibernetico in quanto le infrastrutture ICT sono spesso usate per scopi sia civili sia militari.

L'ultimo aspetto del primo pilastro della Dichiarazione riguarda un tema che ha registrato un diffuso consenso nell'ambito del negoziato internazionale: l'idea che gli Stati debbano adempiere ai loro obblighi internazionali in materia di diritti umani anche nel contesto *cyber*, con particolare rilievo per quanto concerne la libertà di opinione e di espressione, il diritto alla *privacy*, la libertà di cercare, ricevere e rivelare informazioni, la libertà di assemblea e associazione pacifiche, la proibizione delle discriminazioni e i diritti dei bambini.

5. *Segue: c) Il secondo pilastro della Dichiarazione: l'attribuzione della condotta ai fini della responsabilità dello Stato*. – Il secondo pilastro della Dichiarazione è dedicato esclusivamente al tema dell'attribuzione allo Stato della condotta (azione o omissione) internazionalmente illecita ai fini dell'attribuzione della responsabilità. Nella Dichiarazione non è indicato alcun elemento di specificità per quanto concerne la dimensione cibernetica, tant'è che si fa esclusivamente riferimento ad alcune delle regole contenute nel *Progetto di articoli sulla responsabilità degli Stati per atti illeciti internazionali* adottato nel 2021 dalla Commissione del diritto internazionale (CDI) dell'ONU[12].

La Dichiarazione ribadisce, anzitutto, che ai termini del diritto internazionale consuetudinario lo Stato è responsabile per la condotta dei suoi organi e, generalmente, non è responsabile per la condotta di attori non statali non autorizzati a svolgere funzioni di governo. Tuttavia, essa fa poi riferimento agli articoli 8 e 11 del Progetto della CDI: il primo riconosce come attribuibile allo Stato la condotta di attori non statali che hanno agito su sua istruzione o sotto la sua direzione o controllo; il secondo stabilisce che la condotta dell'attore non statale può essere attribuita allo Stato se questo la riconosce e la fa propria.

Nella sostanza, la Dichiarazione non fa che riprendere le principali regole internazionali esistenti nella materia attraverso l'autorevole lavoro della Commissione del diritto internazionale e senza tener conto di aspetti problematici che, anche a questo riguardo, la prassi internazionale ha evidenziato, soprattutto per quanto concerne le condizioni che determinano l'attribuzione allo Stato di condotte svolte sotto la sua "direzione o controllo" da parte di attori non statali.

6. *Segue: d) Il terzo pilastro della Dichiarazione: le risposte degli Stati.* – Nel terzo pilastro la Dichiarazione si occupa delle reazioni degli Stati a operazioni cibernetiche da parte di altri Stati richiamando a regole internazionali ben note e riconosciute. Anzitutto, al *regolamento pacifico delle controversie* con espresso richiamo dell'art. 2, par. 3, della Carta ONU che lo pone tra i principi in base ai quali gli Stati membri devono agire per realizzare i fini dell'Organizzazione. Più specificamente la Dichiarazione richiama anche l'art. 33, par. 1, della Carta, che apre il capitolo VI dedicato, appunto, al regolamento pacifico delle controversie la cui continuazione può mettere in pericolo il mantenimento della pace e della sicurezza internazionali. La disposizione indica tra i mezzi utilizzabili dagli Stati per regolare pacificamente le loro controversie: il negoziato, l'inchiesta, la mediazione, la conciliazione, l'arbitrato, il regolamento giudiziale, il ricorso ad organizzazioni o accordi regionali, o altri mezzi pacifici di loro scelta.

Viene fatto riferimento, poi, alle *ritorsioni* che gli Stati possono adottare per reagire a operazioni cibernetiche illecite di altri Stati. Anche qui si fa ricorso alla nozione di

[12] V. *Report of the International Law Commission*, 53rd session, *UNGA Official Records*, 56th session, Supplement 10, 29.

ritorsione, ben stabilita dal diritto internazionale: un atto ostile che non comporta una violazione di obblighi internazionali.

La Dichiarazione prende in esame anche le reazioni degli Stati ad attacchi *cyber* che, pur non essendo conformi al diritto internazionale, non costituiscono degli illeciti in ragione dell'esistenza di specifiche circostanze. Anche in questo caso si prende come punto di riferimento il Progetto di articoli della CDI citato in precedenza, in particolare gli articoli 20 (consenso dello Stato leso), 21 (legittima difesa), 22 (contromisure), 23 (forza maggiore), 24 (*distress*), e 25 (stato di necessità). Alcune di queste circostanze sono poi trattate specificamente: la legittima difesa, l'invocazione della responsabilità dello Stato, le contromisure e lo stato di necessità. Alla legittima difesa, insieme al divieto dell'uso della forza, dedicheremo alcune riflessioni *ad hoc* in un paragrafo successivo.

Tra le altre circostanze escludenti l'illecito cui la Dichiarazione fa riferimento, ci sembra opportuno qui riprendere quanto indicato rispetto allo *stato di necessità* e alla sua declinazione nel contesto *cyber*. In proposito la Dichiarazione richiama il contenuto dell'art. 25 del Progetto di articoli della CDI il quale prevede che uno Stato può invocare lo stato di necessità come causa di esclusione dell'illiceità di un suo comportamento contrario a un obbligo internazionale se è l'unico modo per salvaguardare un interesse essenziale dello Stato rispetto a un grave e imminente pericolo e lo stesso non danneggia seriamente un interesse essenziale di altri Stati o della Comunità internazionale nel suo insieme. Nel contesto *cyber* un interesse può essere considerato essenziale in ragione della tipologia di infrastruttura critica obiettivo dell'operazione *cyber* e quando tale infrastruttura è rilevante per lo Stato nel suo complesso. Infine, la Dichiarazione fa riferimento a due circostanze che impediscono di invocare lo stato la necessità: quando lo Stato stesso ha contribuito a determinare la situazione di necessità; quando l'obbligo internazionale che si viola esclude la possibilità di invocare la necessità.

7. *L'applicazione dello spazio cibernetico delle regole relative al divieto dell'uso della forza e alla legittima difesa*. – Come già brevemente anticipato, riteniamo utile proporre una specifica riflessione sull'applicazione nello spazio cibernetico del divieto dell'uso della forza e della legittima difesa in ragione dei problemi emersi nel corso del negoziato in sede ONU sulla definizione di un *framework* normativo internazionale in materia di *cybersecurity*. Anche in questo caso partiremo dal contenuto della Dichiarazione del Consiglio dell'UE per poi indicare altre posizioni, di singoli Stati o di organizzazioni regionali, in modo da fornire indicazioni esaurienti sullo stato dell'arte nella materia.

Per quanto concerne il divieto dell'uso della forza, la Dichiarazione UE fa riferimento alle fonti normative pertinenti (e oramai da tempo acquisite): l'art. 2, par. 4, della Carta ONU e la Dichiarazione sulla definizione di aggressione di cui alla risoluzione 3314 del 14 dicembre 1974. C'è poi l'indicazione che il funzionamento delle società moderne è in maniera massiccia legato alle ICT e che queste possono essere distrutte o danneggiate da operazioni cibernetiche senza produrre danni materiali rilevanti, ma con

effetti sfavorevoli su vasta scala anche per quanto concerne lo svolgimento delle normali attività della vita quotidiana.

Secondo la Dichiarazione, l'effetto combinato di diverse operazioni cibernetiche con scopi malevoli potrebbe essere equiparato a un uso della forza nella dimensione cinetica e, quindi, violare il divieto di cui all'art. 2, par. 4 (e dalla norma consuetudinaria cogente corrispondente, ma di ciò il documento UE non parla).

Infine, la Dichiarazione richiama alcune situazioni nelle quali il divieto dell'uso della forza non trova applicazione. In primo luogo, la legittima difesa da esercitare in caso di attacco armato in conformità a quanto previsto dall'art. 51 della Carta ONU e di cui diremo in seguito. La Dichiarazione precisa anche che non tutti gli usi della forza costituiscono un attacco armato. Anche questa ci sembra una precisazione doverosa, in ragione del fatto che solo un uso della forza che raggiunge la soglia dell'attacco armato consente l'esercizio della legittima difesa. In secondo luogo, si fa riferimento all'uso della forza autorizzato dal Consiglio di sicurezza per mantenere o ristabilire la pace e la sicurezza internazionali ai termini del capitolo VII della Carta ONU. Infine, all'uso della forza esercitato con il consenso dello Stato nel territorio dello stesso.

Per quanto riguarda la legittima difesa, la Dichiarazione dà maggiore concretezza a quanto già indicato in precedenza ribadendo che un'operazione cibernetica, la cui portata e i cui effetti sono comparabili a quelli di un'azione militare nel dominio cinetico, può costituire un attacco armato ai termini dell'art. 51 della Carta e, quindi, dare luogo a un'azione in legittima difesa individuale e collettiva. I fattori rilevanti per valutare la portata e gli effetti di un'operazione cibernetica assimilabile a un attacco armato sono costituiti dall'estensione dei danni, dalla distruzione di proprietà, ivi comprese infrastrutture ICT, il ferimento o la morte di persone. La Dichiarazione aggiunge anche che l'uso della forza individuale e collettivo in legittima difesa, per essere considerato legale, deve rispettare i requisiti di necessità e proporzionalità.

In linea generale si tratta di indicazioni corrette, anche se appaiono piuttosto generiche soprattutto in relazione alla gravità dei danni a beni e persone che consentono di determinare l'esistenza dell'attacco armato.

Come anticipato in precedenza, l'applicazione di questi due istituti fondamentali del diritto internazionale contemporaneo anche nello spazio cibernetico è oggetto di un confronto tra gli Stati la cui analisi certamente aiuta a capire la portata degli aspetti problematici che ancora si frappongono al raggiungimento di una posizione comune all'interno dell'ONU in materia di regole internazionali applicabili nello spazio cibernetico.

Partiamo dal divieto dell'uso della forza. Guardando alle posizioni espresse dagli Stati, sia individualmente sia attraverso organizzazioni regionali, è facile constatare l'appoggio ampiamente diffuso all'idea dell'applicazione di tale divieto anche nello spazio cibernetico. In tal senso si esprimono, oltre ai membri dell'UE, anche molti altri Stati occidentali (a titolo di esempio si può fare riferimento alla posizione assunta da

Svizzera[13], Norvegia[14], Canada[15], Nuova Zelanda[16], Australia[17]), gran parte dei Paesi asiatici e del Pacifico (sempre a titolo di esempio si può fare riferimento al Giappone[18] e al Pakistan[19]), i Paesi latino americani (si può prendere in considerazione la posizione del Brasile[20] e quella della Costa Rica[21]) e i Paesi africani (per questi si può richiamare la posizione dell'Unione africana[22]).

Ciò detto, le posizioni degli Stati cominciano a disallinearsi allorché si cerca di precisare gli elementi che caratterizzano l'applicazione del divieto dell'uso della forza nella dimensione cinetica. Proprio la distinzione tra uso della forza vietato dall'art. 2, par. 4, e la nozione di attacco armato di cui all'art. 51, nella loro applicazione nello spazio cibernetico, è uno dei temi che mostra un disallineamento nelle posizioni degli Stati. Alcuni, ad esempio, senza alcun approfondimento particolare, fanno genericamente riferimento all'importanza del divieto *ex* art. 2, par. 4, in relazione alle operazioni cibernetiche[23]. Altri, con maggiore puntualità cercano di porre le basi materiali per operare una distinzione tra divieto dell'uso della forza e attacco armato. Il punto di partenza è il riconoscimento del fatto che un'operazione cibernetica può essere considerata un uso della forza se produce danni e distruzioni analoghi a quelli prodotti da un'operazione condotta con armi convenzionali[24]. Si precisa, poi, che la valutazione va fatta caso per caso tenuto conto degli effetti prodotti dall'operazione cibernetica. In tale prospettiva vengono fatti anche esempi di operazioni cibernetiche che violano il divieto. Sono ritenute tali quelle che causano danni fisici a persone o significative distruzioni di proprietà, nonché quelle che disabilitano permanentemente infrastrutture critiche quali reti elettriche o strutture di servizi idrici e sanitari[25].

L'attacco armato, invece, viene considerato – in linea con la giurisprudenza della Corte internazionale di giustizia[26] – la forma più grave di uso della forza che consente la reazione militare, individuale e collettiva, in legittima difesa. Anche la valutazione dell'esistenza di un attacco armato cibernetico è fatta – secondo gli Stati che si

[13] *Switzerland's Position Paper on the Application of International Law in Cyberspace*, maggio 2021, Annex UNGGE 2019/2021, 4, reperibile *online*.

[14] Cfr. V. Musæus, *Norway's Position Paper on International Law and Cyberspace*, in *Nordic Journal of International Law*, 2023, 470 ss.

[15] Government of Canada, International Law Applicable in Cyberspace, aprile 2022, reperibile *online*.

[16] New Zeland Foreign Affairs and Trade, The Application of International Law to State Activity in Cyberspace, dicembre 2020, reperibile *online*.

[17] 2017 – Australia's Position on the Application of International Law to State Conduct in Cyberspace, e 2019 Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, reperibili *online*.

[18] Japanese Ministry of Foreign Affairs, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, giugno 2021, 6, reperibile *online*.

[19] Pakistan Mission to the United Nations, *Pakistan's Position on the Application of International Law in Cyberspace*, 3 marzo 2023, reperibile *online*.

[20] V. UN Doc. A/76/136 del 13 luglio 2021, 19.

[21] Costa Rican Ministry of Foreign Affairs, *Costa Rica's Position on the Application of International Law in Cyberspace*, 21 luglio 2023, 10-11, reperibile *online*.

[22] African Union - Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, 29 gennaio 2024, 1, reperibile *online*.

[23] Così si esprime il Giappone nel documento cit. a nota 18.

[24] Cfr. le posizioni espresse dalla Costa Rica (cit. a nota 21) e dalla Norvegia (cit. a nota 14).

[25] Cfr, la posizione della Costa Rica, cit.

[26] Ci riferiamo in particolare alla sentenza nel *caso Nicaragua*, Corte internazionale di giustizia, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua c. United States of America)*, in *ICJ Reports*, 1986, 14 ss.

pronunciano sul punto – caso per caso, attraverso la comparazione della portata e degli effetti dello stesso con quelli di un attacco armato cinetico. Secondo alcuni Stati esempi di attacchi armati cibernetici potrebbero essere considerati quelli che causano significative perdite di vite e distruzione di infrastrutture critiche[27].

In linea generale, quindi, la gran parte degli Stati sostiene una interpretazione ampia del divieto dell'uso della forza nella dimensione cibernetica, senza lasciare spazio a eventuali eccezioni tese a restringerne la portata. Allo stesso modo, riconosce la necessità di distinguere tra uso della forza oggetto del divieto e attacco armato.

Non mancano, tuttavia, posizioni specifiche delle quali è necessario tener conto, in quanto si tratta di attori importanti del sistema internazionale: USA, Russia, Cina.

Gli Stati Uniti considerano applicabili alle attività cibernetiche sia il divieto dell'uso della forza *ex* art. 2, par. 4 (e la norma consuetudinaria cogente corrispondente), sia la nozione di attacco armato *ex* art. 51. La reazione militare in legittima difesa deve tener conto della natura e dell'estensione dei danni, delle perdite di vite umane e delle distruzioni di proprietà. C'è da dire che gli USA non danno elementi di maggiore precisione per poter distinguere la violazione del divieto dall'attacco armato che rimettono, probabilmente, alla valutazione dello Stato leso sulla base delle specificità del caso[28].

La Russia nelle sue prese di posizione fa riferimento, in modo alquanto generico, al consenso raggiunto dalla Comunità internazionale sull'applicabilità al dominio cibernetico dei principi fondamentali della Carta dell'ONU, tra i quali il divieto dell'uso della forza. Tuttavia, in ragione delle specificità dello "information environment" e del fatto che le attività ivi condotte possono essere anonime, la Russia ritiene che l'applicazione in tale ambiente delle regole del diritto internazionale esistenti non può essere automatica e sottolinea la necessità di discutere in modo approfondito i problemi che si pongono in modo da favorire l'elaborazione di un approccio universale sotto gli auspici dell'ONU[29].

Significativa e in parte analoga a quella russa è la posizione espressa dalla Cina che fa riferimento, anzitutto, alla necessità che gli Stati agiscano nello spazio cibernetico in modo coerente con l'obiettivo di mantenere la pace e la sicurezza internazionali. In secondo luogo, fa riferimento ai principi della Carta dell'ONU, ivi compreso il divieto della minaccia dell'uso della forza, sostenendone l'applicazione anche nello spazio cibernetico. Tuttavia, aggiunge anche che gli Stati devono agire con "prudenza" rispetto all'applicazione del diritto dei conflitti armati e dello *ius ad bellum* «and prevent escalation of conflicts or turning cyberspace into a new battlefield». Inoltre, non viene esclusa la necessità – per garantire una pace duratura e la stabilità nello spazio cibernetico

[27] Anche in questo caso ci riferiamo alla posizione della Costa Rica e della Norvegia citate in precedenza.
[28] V. UN Doc. A/76/136, cit., 136 ss.
[29] Ivi, 79 ss.

– di elaborare nuovi strumenti giuridici adeguati alla specificità e all'evoluzione delle ICT e fondati su un'ampia partecipazione di tutti gli Stati[30].

La tendenza, nelle posizioni degli Stati indicate, a favore del divieto dell'uso della forza si registra anche per quanto concerne la legittima difesa. In linea di massima riteniamo di poter dire che la posizione prevalente è quella degli Stati che sostengono che una o più operazioni cibernetiche possano raggiungere la soglia dell'attacco armato e quindi dare luogo alla reazione in legittima difesa sia individuale sia collettiva. Analogo supporto è rilevabile rispetto all'idea che l'attività *cyber* costituisce un attacco armato quando è attribuibile a uno Stato e ha una portata e produce effetti equivalenti a un attacco cinetico[31]. Va detto, tuttavia, che non mancano posizioni più prudenti e che sottolineano l'esigenza di un'attenta e circostanziata valutazione di tutti gli elementi che possono contribuire portata e effetti dell'attacco armato in campo cibernetico[32].

Un diffuso sostegno si registra sul fatto che l'azione in legittima difesa anche nel dominio *cyber* va condotta nel rispetto dei requisiti di necessità e proporzionalità[33].

Non mancano, poi, gli Stati che sostengono la legalità dell'azione "anticipata" nell'imminenza di un attacco cibernetico che si suppone possa avere un impatto sufficientemente grave[34]. Anche se va detto che altri Stati ritengono che la legittima difesa sia consentita solo in caso di attacco armato cibernetico in corso e che la legittima difesa "anticipata" o "preventiva" necessiti di ulteriori approfondimenti[35].

Anche nel caso della legittima difesa ci troviamo quindi di fronte a posizioni che, nel complesso, esprimono la problematicità che si accompagna all'applicazione di tale istituto nello spazio cibernetico, non diversamente da quanto succede rispetto alla dimensione cinetica. La qual cosa fa emergere l'importanza di un approccio prudente alla materia e, probabilmente, la necessità di approfondire ulteriormente la discussione e il confronto tra gli Stati.

8. *Conclusioni*. – La Dichiarazione del Consiglio dell'UE sul diritto internazionale applicabile nello spazio cibernetico è certamente un documento importante, soprattutto perché costituisce una testimonianza della volontà degli Stati membri di agire in modo unitario nel contesto del negoziato in ambito ONU.

A fronte di ciò non si può fare a meno di rilevare che il documento, su tutti i temi trattati, si limita a ribadire il diritto internazionale esistente e la sua applicabilità nello spazio cibernetico, senza tenere conto che non sempre ciò è possibile e che la portata di

[30] Chinese Ministry of Foreign Affairs, *China's Positions on International Rules-Making in Cyberspace*, ottobre 2021, reperibile *online*.

[31] A titolo di esempio si rinvia alla posizione della Nuova Zelanda (cit., nota 16), dell'Australia (cit., nota 17) e della Svizzera (cit., nota 13).

[32] Per tutti v. la posizione espressa dall'Unione africana, cit., nota 22.

[33] Sempre a titolo di esempio si rinvia alla posizione espressa da Brasile, cit., nota 20.

[34] V. le posizioni espresse da Nuova Zelanda (cit., nota 16), Australia (cit., nota 17) e Stati Uniti (cit., nota 28).

[35] V. la posizione espressa dall'Unione africana (cit., nota 22).

alcune delle norme prese in considerazione è controversa finanche nella dimensione cinetica.

Rispetto alla definizione di un quadro normativo internazionale nella materia, la cosa che maggiormente preoccupa è che l'approccio della Dichiarazione, con il mancato riconoscimento della problematicità di alcuni istituti del diritto internazionale nello spazio cibernetico, possa costituire un ostacolo al dialogo e al confronto con altri attori rilevanti nel contesto del negoziato.

Marzo 2025