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

Il ruolo e le attività del Consiglio di sicurezza dell'ONU in materia di *cybersecurity*

Pietro Gargiulo
Professore ordinario di Diritto internazionale, Università degli Studi di Teramo – Direttore responsabile della Rivista della SIOI "La Comunità Internazionale"

Premessa. Da diverso tempo, l'ONU, la principale organizzazione internazionale di carattere universale attualmente esistente, si sta occupando del tema della *cybersecurity*. È facile comprendere che l'Organizzazione costituisce un punto di riferimento di assoluto rilievo per tutti coloro che sono interessati a studiare l'evoluzione delle iniziative dirette a elaborare e approvare il quadro normativo internazionale applicabile alle operazioni degli Stati – ma anche degli attori non statali – nello spazio cibernetico. Ciò in quanto rappresenta il contesto più adeguato per conoscere e valutare le posizioni degli attori più rilevanti della Comunità internazionale, ivi compresi gli Stati "forti" del sistema internazionale – gli Stati Uniti, la Cina, la Russia – i cui interessi contrastanti in materia di *cybersecurity* sono all'origine delle difficoltà che attualmente caratterizzano l'adozione di regole comuni in questo nuovo dominio.

Nell'ambito dell'ONU il tema della *cybersecurity* è principalmente esaminato nel quadro degli sviluppi delle tecnologie dell'informazione e delle comunicazioni (ICT, secondo l'acronimo dall'inglese) e il loro impatto sulla sicurezza internazionale. È piuttosto chiaro, da ciò, il legame tra uso delle ICT e il fine principale dell'ONU, il mantenimento della pace e della sicurezza internazionali. In effetti, l'uso corretto delle ICT è capace di garantire enormi benefici economici, sociali, culturali, civili e politici. Tuttavia, è da tenere presente anche lo sviluppo senza precedenti di attività malevole o addirittura criminali attraverso le ICT, molto spesso nel contesto di conflitti internazionali e interni, contro infrastrutture critiche (sanitarie, finanziarie, energetiche, satellitari, trasporti e altro) e la loro estrema pericolosità specialmente nel contesto di attacchi informatici simultanei.

Le attività appena indicate possono incidere notevolmente in maniera negativa sul mantenimento della pace e della sicurezza internazionali. Da ciò l'esigenza di promuovere l'adozione di un quadro comune di regole internazionali nella materia capaci di favorire gli effetti positivi dell'uso delle ICT e contrastarne gli usi malevoli. Di questi aspetti si occupa l'ONU principalmente attraverso le attività dell'Assemblea generale, l'istituzione dell'Organizzazione nella quale sono rappresentati tutti gli Stati membri[1]. Sin dal suo primo intervento nella materia, verso la fine degli anni '90 del Novecento, l'Assemblea esprimeva preoccupazione per gli usi delle ICT contrari all'obiettivo del mantenimento della pace e della sicurezza internazionali e indicava la volontà di favorire il dialogo tra gli Stati membri per favorire l'identificazione delle regole del diritto internazionale applicabili nell'uso delle ICT.

[1] Sulle attività in questione si rinvia a 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. e i lavori ivi citati.

Più recentemente anche il Consiglio di sicurezza si è occupato del tema dell'uso delle ICT e dell'eventuale impatto sotto il profilo del mantenimento della pace e della sicurezza internazionale[2]. Su questi aspetti il Consiglio è intervenuto sia nel contesto dell'esame di temi di più ampia portata sia attraverso incontri informali specificamente dedicati ai temi della *cybersecurity*. Nelle pagine che seguono ci soffermeremo su tali iniziative per cercare di capire i possibili approdi del dialogo/confronto tra gli Stati membri all'interno dell'organo mondiale che, ai termini dell'art. 24 della Carta, detiene la "responsabilità principale" per il mantenimento della pace e della sicurezza internazionali.

Il tema della *cybersecurity* nel contesto di dibattiti del Consiglio di sicurezza su questioni di carattere generale. Come indicato in precedenza, il Consiglio di sicurezza ha avuto modo di occuparsi del tema della *cybersecurity* nel contesto di riunioni dedicate ad altre questioni, soprattutto di carattere generale e comunque non specificamente dedicate al tema. È chiaro che, in tali contesti, gli Stati partecipanti alla discussione non hanno approfondito il tema dal punto di vista tecnico, ma certamente hanno avuto l'opportunità di chiarire le loro posizioni nella materia e indicato le strategie ritenute più idonee ad affrontare le sfide alla pace e alla sicurezza poste dalle attività degli Stati in questo nuovo dominio.

Un esempio rilevante riteniamo possa essere costituito dal dibattito ministeriale tenutosi in Consiglio di sicurezza nel 2019 sotto il punto in agenda "Maintenance of international peace and security, Challenges to peace and security in the Middle Est". All'incontro, promosso dalla Polonia e svoltosi il 20 agosto, partecipavano, tra gli altri, numerosi Stati della regione e i rappresentanti dell'Unione europea e della Lega degli Stati arabi presso le Nazioni Unite[3].

La "concept note" preparata dalla Polonia per l'incontro, oltre a fare riferimento al contesto storico che caratterizza il lungo conflitto nella regione Medio-orientale, indicava lo scopo dell'incontro nell'individuazione, attraverso il confronto e la discussione, delle misure concrete affinché i Paesi dell'area fossero in grado di affrontare le cause profonde delle crisi in Medio Oriente[4]. A tal fine, il documento polacco poneva una serie di domande a cui gli Stati avrebbero dovuto dare una risposta e, tra queste, era anche chiesto «How to counteract cyber threats, including threats to energy infrastructure, in terms of promoting cooperative mechanisms for deterring and responding to significant cyber incidents in the Middle East?»[5].

In verità, nel corso del dibattito non furono in molti ad affrontare le tematiche che qui interessano. In aggiunta a quanto indicato nella "concept note", il Rappresentante della Polonia sottolineava che la sicurezza nello spazio cibernetico costituiva una sfida centrale e che il rafforzamento della "cyberstability" regionale dipendeva dall'assunzione di comportamenti responsabili nello spazio cibernetico da parte di tutti gli Stati del Medio

[2] In generale sul ruolo del Consiglio di sicurezza e il tema della *cybersecurity* si rinvia a UNIDIR, *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century*, Unidir Resources, 2017, reperibile *online*; E. Tikka, N.N. Schia, *The Role of the Security Council in Cybersecurity. International Peace and Security in Digital Age*, in E. Tikka, M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity*, Abingdon/New York, 2020, 354 ss.

[3] Il verbale della riunione del Consiglio è in UN Doc. S/PV.8600.

[4] V. UN Doc. S/2019/643 del 6 agosto 2019.

[5] Ivi, 4.

Oriente. Per favorire ciò, il Rappresentante della Polonia faceva riferimento al "Warsaw Process" per promuovere un futuro di pace e sicurezza in Medio Oriente"[6], avviato nel 2019 in collaborazione con gli Statu Uniti e nel cui ambito era stata prevista la creazione di gruppi di lavoro che, tra le altre cose si occupavano anche di *cybersecurity*[7].

È opportuno sottolineare che il gruppo di lavoro sulla *cybersecurity* si riunì nella Repubblica di Korea il 7 e 8 ottobre 2019 e adottò uno "statement"[8] nel quale si sottolinea soprattutto l'avvenuta discussione sui meccanismi cooperativi per rispondere a significativi incidenti *cyber*. In particolare, il confronto tra i rappresentanti degli Stati era avvenuto sulla cruciale importanza di condividere le *best practices* in materia di *cybersecurity*, sullo sviluppo delle capacità di risposta agli incidenti *cyber*, sulla lotta alla criminalità cibernetica, tenuto conto della Convenzione di Budapest[9], sullo sviluppo e l'attuazione di strategie nazionali nella materia.

Inoltre, di notevole importanza nello *statement* è anche il riferimento alle iniziative condotte dall'ONU, in particolare dall'Assemblea generale, sull'adozione di un framework per la stabilità nello spazio cibernetico i cui tre elementi di riferimento sono: l'affermazione dell'applicabilità di tutte le regole di diritto internazionale ai comportamenti degli Stati nello spazio cibernetico; l'adesione volontaria alle "non-binding norms" sui comportamenti responsabili degli Stati nello spazio cibernetico in tempo di pace; l'analisi, lo sviluppo e l'attuazione di misura di rafforzamento della fiducia tra gli Stati per ridurre il rischio di conflitti nel *cyberspace*.

Ritornando al dibattito nel Consiglio di sicurezza relativo al Medio Oriente merita di essere richiamato l'intervento del Rappresentante saudita che elencava i *cyberattacks* contro infrastrutture critiche tra le minacce e le interferenze agli affari interni degli Stati che impediscono l'instaurazione del dialogo e favoriscono, invece, la realizzazione di scopi egemonici o espansionisti[10].

L'Iran preferiva concentrare l'attenzione sulle accuse agli Stati Uniti di appoggiare l'occupazione illegale della Palestina, di essere responsabile dei principali conflitti nella regione (Iraq, Siria, Yemen) e di essere coinvolto nell'appoggio a gruppi di terroristi e in molti altri atti illegali, ivi compresi gli attacchi cibernetici in Medio Oriente[11].

Con maggiore puntualità il tema è invece affrontato dal Rappresentante del Qatar che identifica la *cybersecurity* come una sfida "enorme" soprattutto perché, quando le potenzialità della tecnologie informatiche sono utilizzate per scopi malevoli, possono destabilizzare le relazioni e la sicurezza internazionali. In particolare, il Rappresentante del Qatar dichiara che «l'assenza di istituzioni e normative internazionali per governare questo fondamentale settore richiede l'adozione di misure severe nei confronti dei

[6] Maggiori informazioni sul "Warsaw Process" possono essere recuperate sul sito www.gov.pl/diplomacy/warsaw-process.

[7] Per l'intervento del Rappresentante della Polonia v. il documento cit. alla nota 3, 5. Anche il Rappresentante degli Stati Uniti faceva riferimento nel suo intervento al "Warsaw Process", ivi, 6.

[8] Lo "statement" è reperibile online a www.gov.pl/diplomacy/warsaw-process-cybersecurity-working-group-convenes-in-seoul.

[9] La Convenzione di Budapest è stata adottata nell'ambito del Consiglio d'Europa nel 2001 ed è uno strumento fondamentale per aiutare gli Stati parti a elaborare legislazioni per combattere il fenomeno della criminalità informatica e per favorire la cooperazione internazionale nella materia. Nel 2003 si è anche arricchita di un Protocollo sugli atti di natura razzista e xenofoba a mezzo di sistemi informatici.

[10] Per l'intervento dell'Arabia Saudita v. il documento cit. alla nota 3, 31.

[11] Ivi, 33.

responsabili dei reati informatici, tra le quali quelle dirette a renderli responsabili legalmente degli stessi con l'aggiunta di sanzioni adeguate»[12].

Le iniziative del Consiglio sulla *cybersecurity* secondo l'*Arria-formula meetings*. I limiti istituzionali e normativi internazionali nel campo della *cybersecurity* sono apparsi evidenti nel recente susseguirsi di numerosi *cyberattacks* che hanno reso ancora più evidenti le pericolose conseguenze degli stessi per la stabilità e la pace internazionali. Ciò ha spinto i membri del Consiglio di sicurezza a incrementare la discussione il confronto su tali temi, soprattutto attraverso gli incontri secondo la c.d. "formula Arria".

Come è noto, gli "Arria formula meetings" costituiscono una pratica avviata nel 1992 dall'allora presidente del Consiglio di sicurezza, l'Ambasciatore venezuelano Diego Arria. Si tratta di incontri informali aperti, promossi da uno o più membri del Consiglio di sicurezza per consultare, ascoltare l'opinione e ricevere informazioni da parte di individui, organizzazioni non governative e altre istituzioni su questioni relative al mantenimento della pace e della sicurezza internazionali[13].

Diversi sono gli incontri organizzati dal Consiglio secondo la formula Arria sul tema oggetto di questo lavoro e di cui daremo conto qui di seguito. Un primo incontro rilevante si è avuto il 28 novembre 2016 ed è stato organizzato dalla Spagna e dal Senegal per discutere, in generale, delle sfide alla pace e alla sicurezza derivanti dall'utilizzo delle ICT[14]. Nel corso dell'incontro furono evidenziati i pericoli derivanti dagli attacchi cibernetici e messe in luce le difficoltà per contrastarli e per identificarne i responsabili. Nel corso dell'incontro gli Stati membri furono sollecitati, da un lato, a stabilire delle strategie nazionali per prevenire gli attacchi cibernetici e, dall'altro, a rafforzare la cooperazione internazionale nella materia coinvolgendo tutti gli attori interessati: governi, imprese, organizzazioni regionali e sub-regionali, associazioni rappresentative della società civile.

Un nuovo incontro secondo la formula Arria si tenne nel marzo 2017, questa volta dedicato alle guerre ibride e alle minacce alla pace e alla sicurezza internazionali. L'incontro si rivelò particolarmente interessante almeno sotto due aspetti: il primo concerne l'identificazione dei fattori caratterizzanti la guerra ibrida (sistemi di armi avanzati, attacchi cibernetici, interferenza con processi politici, disseminazione sistematica di propaganda sul piano interno e internazionale, operazioni segrete di *intelligence*, solo per fare alcuni esempi); il secondo riguarda l'idea che la guerra ibrida comporta azioni che ricadono al di sotto della soglia dell'azione militare e ciò al fine di negare o delegittimare la reazione militare da parte del soggetto che subisce le azioni[15].

Successivamente, il Consiglio di sicurezza ha intensificato i suoi lavori sull'impatto della *cybersecurity* sui temi relativi alla pace e alla sicurezza internazionali. Merita di essere qui segnalato, anzitutto, l'incontro organizzato dall'Estonia il 22 maggio 2020, sempre secondo la formula Arria, sul tema "Cyber stability, Conflict prevention and Capacity Buiklding". Secondo quando indicato nella *concept note* estone l'obiettivo

[12] Ivi, 43-44.

[13] V. *UN Security Council Working Methods: Arria-formula Meetings*, www.securitycouncilreport.org del 16 dicembre 2020.

[14] *Open Arria-formula Meeting on Cybersecurity*, What's in Blu, www.securitycouncilreport.org del 25 novembre 2016.

[15] *In Hindsight: The security Council and Cyber Threats*, www.securitycouncilreport.org, January 2020 Monthly Forecast, posted December 23, 2019.

dell'incontro era quello di aumentare la consapevolezza sulle sfide poste dalle attività nello spazio cibernetico alla pace e alla sicurezza internazionali e favorire la discussione a tutti i livelli – globale, regionale e nazionale – sui meccanismi esistenti per mitigare gli attacchi cibernetici e promuovere comportamenti responsabili da parte degli Stati[16]. In verità, in quell'occasione il confronto tra gli Stati e gli altri attori interessati fu fortemente condizionato dalle vicende legate all'aggressione russa dell'Ucraina del febbraio 2022. Infatti, nel corso dell'incontro l'Ucraina accusò la Russia di aver posto in essere "un'aggressione ibrida" nei suoi confronti e sollecitò l'adozione di adeguate misure di *enforcement* per perseguire gli organizzatori e gli autori degli attacchi cibernetici. La Russia, dal canto suo, non partecipò al dibattito e denunciò in uno *statement* che una minoranza di Stati stavano attivamente cercando di perseguire l'obiettivo di militarizzare lo spazio cibernetico e di sfruttare qualsiasi pretesto per giustificare l'adozione di misure unilaterali, ivi compreso l'uso della forza[17].

Pochi mesi dopo, il 26 agosto 2020, anche l'Indonesia organizzò un "Arria-formula meeting", questa volta dedicato ai "Cyber-Attacks against Critical Infrastructures". La *concept note* dell'Indonesia metteva in rilievo, anzitutto, l'importanza assunta dalle ICT sia per il settore pubblico sia per quello privato, rilevando, tuttavia, i rischi potenziali di un loro uso malevolo. In connessione a ciò il documento sottolineava la particolare vulnerabilità delle infrastrutture critiche e la necessità di proteggerle dagli attacchi cibernetici. Parallelamente veniva messo in evidenza la pressante necessità di stabilire dei quadri normativi nazionali e internazionali per garantire comportamenti responsabili degli Stati nell'uso delle ICT[18]. Nel corso del dibattito numerosi Stati si pronunciarono favorevolmente rispetto all'applicazione del diritto internazionale allo spazio cibernetico in tempo di pace. Ma non mancarono significative divergenze rispetto all'applicazione delle norme del diritto internazionale dei conflitti armati[19].

L'incontro più recente del Consiglio di sicurezza sul tema della *cybersecurity*, sempre secondo la formula Arria, si è tenuto il 4 aprile 2024, è stato organizzato dalla Repubblica di Corea, con il supporto di Giappone e Stati Uniti, e si è occupato del tema "Evolving Cyber Threat Landscape and Its Implications for the Maintenance of International Peace and Security".

La *concept note* preparata dalla Corea fa anzitutto riferimento all'evoluzione del panorama delle minacce cibernetiche sottolineando la pericolosità della proliferazione dei "ransomware" (programmi informatici dannosi), l'uso scorretto di criptovaluta, l'aumento di attori non statali malevoli. A fronte di tali fenomeni, gli obiettivi che il *meeting* si è posto sono i seguenti: aumentare la consapevolezza degli Stati membri dell'Organizzazione sul panorama delle attuali minacce cibernetiche e il loro potenziale impatto sul settore pubblico e su quello privato; promuovere una maggiore comprensione dell'impatto sulla pace e la sicurezza internazionali delle attività *cyber* malevole; discutere ed elaborare raccomandazioni sul rafforzamento del ruolo del Consiglio di sicurezza e sul suo impegno nel contrastare la multiforme natura delle minacce cibernetiche.

[16] V. UN doc. S/2020/389 del 12 maggio 2020.

[17] *In Hindsight: The Security Council and Cyber Threats, an Update*, www.securitycouncilreport.org.

[18] *Arria-formula Meeting on Cyber Attacks Against Critical Infrastructures*, What's in Blue, www.securitycouncilreport.org, 24 agosto 2020.

[19] *In Hindsight: The Security Council and Cyber Threats, an Update*, cit.

Nel corso del dibattito numerosi rappresentanti degli Stati membri hanno evidenziato i pericoli derivanti dall'emergere di nuove minacce cibernetiche e dall'evoluzione di quelle già esistenti[20]. Come pure non sono mancati riferimenti all'uso malevolo degli strumenti cibernetici da parte di criminali e terroristi. Particolarmente interessanti risultano i numerosi riferimenti dei rappresentanti degli Stati membri al fatto che il diritto internazionale e la Carta dell'ONU sono applicabili allo spazio cibernetico e devono essere rispettati. Sotto questo profilo va, tuttavia, menzionata la posizione della Russia che ha ritenuto la discussione del tema della *cybersecurity* nel Consiglio di sicurezza una inutile duplicazione delle attività condotte in altri organi dell'ONU.

Conclusioni. È facile constatare che il tema della *cybersecurity* è oggetto di una particolare attenzione nel contesto dell'ONU considerata l'importanza che esso riveste sotto diversi profili inerenti ai pilastri di attività dell'Organizzazione.

L'impatto della *cybersecurity* sul mantenimento della pace e della sicurezza internazionali solleva complesse e delicate questioni perlopiù attinenti alla necessità di trovare un accordo tra gli Stati membri sul quadro normativo internazionale applicabile allo spazio cibernetico. Sotto questo profilo è noto che da diverso tempo è aperto un confronto in Assemblea generale che non ha prodotto i frutti sperati. Infatti, ancora persistono divisioni, talvolta profonde, tra gli Stati membri: da un lato, coloro (e si tratta di una cospicua maggioranza) che ritengono che le regole del diritto internazionale attualmente in vigore per quanto concerne il mantenimento della pace e della sicurezza internazionali siano applicabili anche nello spazio cibernetico; dall'altro, coloro (una minoranza certamente, ma con significative presenze quali la Cina e la Russia) che ritengono che la discussione intorno al regime di regole applicabili allo spazio cibernetico vada ulteriormente approfondita.

Che anche il Consiglio di sicurezza abbia incominciato ad occuparsi attivamente della questione è certamente un fatto positivo, sebbene attraverso l'*Arria-formula meeting* che, com'è noto, è un contesto informale per il confronto tra gli Stati membri soprattutto con portatori di interessi di varia natura. Le prese di posizione degli Stati membri in occasione di tali confronti rispecchiano sostanzialmente le divisioni che si sono in precedenza indicate e non mostrano spiragli per un riavvicinamento. D'altra parte, è da tenere presente che il momento internazionale attuale, i conflitti gravissimi che lo stanno caratterizzando, non favoriscono l'avvio di una fattiva forma di cooperazione internazionale in questo ambito.

Ottobre 2024

[20] Il dibattito può essere ascoltato su https://webtv.un.org/en/asset/k1q/k1qmd5ya35.