NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

Il Position Paper della Germania sull'applicazione del diritto internazionale nel cyberspazio e il rapporto finale dell'Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*

di Flavia Zorzi Giustiniani**

Il 5 marzo scorso la Germania ha pubblicato un ***position paper*** **intitolato "On the application of International Law in Cyberspace"**. Così facendo lo Stato tedesco è intervenuto, seguendo un modus operandi già utilizzato da diversi Stati in tempi recenti[1], per dare il proprio contributo unilaterale su di un tema rimasto a lungo in fase di stallo nelle negoziazioni intraprese a livello multilaterale. L'obiettivo è in verità duplice: contribuire all'attuale dibattito relativo alle modalità di applicazione del diritto internazionale nel contesto cibernetico e favorire la trasparenza, la comprensibilità e la certezza del diritto con riguardo ad un importante aspetto della politica estera[2]. Il documento, realizzato congiuntamente dai ministeri degli affari esteri, della difesa e degli interni, parte dal presupposto sempre meno controverso che il diritto internazionale è applicabile in materia, per poi delineare le modalità di tale applicazione con specifico riferimento agli obblighi derivanti dalla Carta delle Nazioni Unite, al diritto internazionale umanitario e alla responsabilità internazionale dello Stato.

Il documento dichiara anzitutto che il principio della sovranità statale si applica alle attività degli Stati nel cyberspazio e che le operazioni cibernetiche attribuibili a Stati che violano la sovranità di un altro Stato sono contrarie al diritto internazionale[3]. Viene tuttavia precisato che

---

* Contributo sottoposto a *peer review*.

** Ricercatrice di Diritto internazionale presso l'Università Telematica Internazionale UNINETTUNO.

[1] Si vedano tra gli altri i *position papers* di Regno Unito (Attorney General Jeremy Wright QC MP, Cyber and international law in the 21st century, 23 maggio 2018, disponibile al link https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century), Paesi Bassi (Minister of Foreign Affairs, Letter to the parliament on the international legal order in cyberspace, 5 luglio 2019, disponibile al link https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace), Francia (Ministère des Armées, International law applied to operations in the cyberspace, 9 settembre 2019, disponibile al link https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf) e Nuova Zelanda (New Zealand Government, The application of international law to State activity in Cyberspace, 1° dicembre 2020, disponibile al link https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf).

[2] Cfr. The Federal Government, "On the application of International Law in Cyberspace", 5 marzo 2021, disponibile al link https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf, pp. 1-2.

[3] Si tratta di un'opinione già espressa, *inter alia*, dal Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, seconda edizione, Cambridge University, Press, 2017, regola 4.

ISSN 2279-7238

in caso sia di effetti e di danni fisici nel territorio di un altro Stato che di danni funzionali ("functional impairments") a infrastrutture cibernetiche al di sotto di una certa soglia, ossia quando tali conseguenze sono "negligible", non vi è violazione della sovranità territoriale[4]. Si specifica poi che non è sufficiente che l'obiettivo dell'operazione ostile sia una "critical infrastructure" o una compagnia di speciale interesse pubblico situata sul territorio dello Stato giacché manca una definizione uniforme di tali termini a livello internazionale[5].

Malgrado l'assenza di unanimità sul punto da parte degli Stati[6], la Germania afferma nel documento che il principio di *due diligence* si applica nel contesto cibernetico e che tale principio ha un particolare rilievo a causa dell'ampia interconnessione dei sistemi e delle infrastrutture cibernetiche[7].

Con riguardo al divieto di intervento illecito, visto come corollario del principio di sovranità, il documento afferma che le misure cibernetiche possono costituire un intervento proibito ai sensi del diritto internazionale se sono comparabili per portata ed effetti alla coercizione in contesti non cibernetici[8]. La coercizione secondo la Germania implica che i processi interni di uno Stato riguardanti aspetti relativi al suo dominio riservato sono significativamente influenzati o bloccati, e che la volontà dello Stato è manifestamente piegata dalla condotta dello Stato straniero. Per potersi qualificare come coercizione, tuttavia, è necessario che lo Stato che agisce intenda intervenire negli affari interni dello Stato colpito. Utilizzando come esempio le interferenze nei processi elettorali tramite attività cibernetiche dannose, la Germania indica come possibili casi di interventi coercitivi sia la diffusione di informazioni via internet che possano incoraggiare rivolte popolari violente che la disattivazione di infrastrutture e tecnologie elettorali quali le schede elettroniche. Altre attività che per portata ed effetti potrebbero essere comparabili alla coercizione sono poi quelle che sono volte e si risolvono in un disturbo significativo o addittittura in un cambiamento permanente del sistema politico dello Stato colpito. Anche con riguardo alla coercizione, dunque, sono gli effetti e non l'obiettivo a determinare l'eventuale contrarietà di una certa attività al diritto internazionale. La Germania conclude tuttavia che a causa della complessità e della singolarità dei suddetti scenari sia difficile formulare dei criteri astratti.

Per quanto attiene alla questione dell'attribuzione di operazioni cibernetiche, il documento afferma anzitutto che (anche) le operazioni cibernetiche *ultra vires*, che siano condotte da organi statali ex art. 14 del Progetto di Articoli sulla Responsabilità degli Stati[9] o da persone o entità incaricate dal diritto di esercitare elementi di autorità governativa ex art. 5 del medesimo progetto,

[4] Cfr. The Federal Government cit., p. 4.
[5] *Ibid.*
[6] Nel Rapporto del 2015 del Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security tale principio è elencato tra le "*voluntary, non-binding* norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment" (Assemblea Generale ONU, A/70/174, 22 luglio 2015, par. 13 c), corsivo nostro).
[7] Cfr. The Federal Government cit., p. 3.
[8] *Ibid.*, p. 5.
[9] Cfr. Commissione del Diritto Internazionale (CDI), Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, in: Report of the International Law Commission on the work of its fifty-third session, 23 April – 1 June and 2 July – 10 August 2001, Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 10, UN Doc. A/56/10.

ISSN 2279-7238

sono attribuibili allo Stato[10]. Di rilievo è poi il fatto che la Germania prenda posizione con riguardo a due questioni assai cruciali e controverse. La prima concerne l'utilizzo remoto di infrastrutture informatiche situate nel territorio di uno Stato (*forum State*) da parte di un altro Stato (Stato agente) per l'attuazione di operazioni informatiche dannose da parte di quest'ultimo. Al riguardo la Germania avverte che se il primo Stato fornisce attivamente e consapevolmente allo Stato agente l'accesso alla sua infrastruttura informatica, così facilitando le operazioni informatiche dannose dallo stesso compiute, sarà responsabile per il suo "aid and assistance"[11]. La seconda questione riguarda il caso in cui uno Stato agisca per via mediata, servendosi di attori non statali. Il Progetto sulla responsabilità degli Stati prevede che uno Stato sia responsabile se un attore non statale agisce su sue istruzioni o sotto la sua direzione o controllo[12]. Applicando tale regola al contesto cibernetico, la Germania precisa che, benché un certo grado di controllo sia necessario, lo Stato non deve avere una visione dettagliata o influenzare tutti i dettagli, in particolare quelli di natura tecnica, dell'operazione[13].

Con riguardo all'atto formale di attribuire una specifica operazione cibernetica dannosa ad uno Stato, il documento precisa che si tratta anzitutto di una prerogativa nazionale. Non è richiesto allo Stato di rendere pubblici i fatti sui quali tale attribuzione è basata, nondimeno la stessa dovrebbe avvenire solo allorché vi sia un grado sufficiente di certezza giacché, come sancito nel rapporto del 2015 dello United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE), le accuse di "cyber-related misconduct" da parte di uno Stato dovrebbero essere motivate[14].

Il documento analizza poi le tre opzioni di risposta non coercitiva disponibili avverso operazioni informatiche dannose, ovvero le ritorsioni, le contromisure e lo stato di necessità. Con riferimento alle contromisure, dopo aver chiarito che tali misure possono essere anche non "cyber-related" e che le condizioni di applicazione sono quelle stabilite nel Progetto di Articoli della CDI, avverte che le contromisure cibernetiche sono suscettibili in particolar modo di generare effetti indesiderati o addirittura illegali. Pertanto gli Stati devono verificare scrupolosamente se siffatte contromisure rispettano i criteri di limitazione. Quanto allo stato di necessità, il documento stabilisce tra l'altro che l'interesse essenziale in gioco può essere riferito al tipo di infrastruttura interessata o al tipo di danno effettivamente o potenzialmente causato dall'operazione cibernetica dello Stato straniero[15]. Un esempio del primo tipo è quello di infrastrutture sensibili, del secondo un danno fisico grave ad individui[16].

Tra le altre questioni su cui il Paper prende posizione è importante menzionare l'applicabilità del diritto internazionale umanitario al cyberspazio. Tale posizione, infatti, è avversata da diversi Stati, *in primis* la Cina e la Russia tanto che queste ultime hanno impedito al GGE di menzionare

[10] Cfr. The Federal Government cit., p. 10.
[11] Cfr. l'art. 16 dei Draft Articles on State Responsibility. V. anche la regola 18 a) del Tallinn Manual 2.0.
[12] Cfr. l'art. 8 dei Draft Articles on State Responsibility.
[13] Cfr. The Federal Government cit., p. 11.
[14] Cfr. A/70/174, par. 28 f).
[15] Cfr. The Federal Government cit., p. 14.
[16] *Ibid.*, p. 14-15.

ISSN 2279-7238

il diritto umanitario nel suo sesto rapporto[17]. Su aspetti più specifici del diritto umanitario la posizione tedesca è nel complesso assai conforme a quella dei suoi alleati della NATO e dell'Unione europea, pur distinguendosi per la meticolosità con cui diverse questioni sono affrontate[18].

Nel concludere, il Paper sottolinea che le incertezze nell'applicazione del diritto internazionale al contesto cibernetico possono e devono essere affrontate facendo ricorso ai metodi di interpretazione consolidati del diritto internazionale[19]. Auspica infine che gli Stati tengano conto dei ricchi e multiformi dibattiti accademici e della società civile sul ruolo e la funzione del diritto internazionale nel contesto cibernetico[20].

Un secondo sviluppo importante in materia é costituito dal **rapporto finale dell'Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)**, pubblicato il 10 marzo scorso[21]. Tale rapporto, che ha visto la luce dopo due anni di deliberazioni, è stato approvato da ben 193 Paesi, che per la prima volta hanno accettato una serie di norme di comportamento responsabile nel cyberspazio.

A differenza del GGE, composto da una ristretta cerchia di delegati governativi[22], l'OEWG è aperto a tutti gli Stati ed ad attori non-statali quali imprese, ONG e accademici ed è stato istituito dalla stessa Assemblea nel dicembre 2018 nell'intento di condurre ulteriori ricerche e di superare i dissensi tra gli Stati[23]. I lavori di entrambi i gruppi sono finalizzati da un lato ad estendere l'applicazione delle regole del diritto internazionale al *cyberspazio* e dall'altro a stabilire nuove regole comuni.

Il rapporto dell'OEWG invero non è giuridicamente vincolante né il suo contenuto è particolarmente innovativo. Nondimeno, la sua adozione segna una svolta epocale giacché è il risultato di un processo negoziale aperto a tutti gli Stati della comunità internazionale e rappresenta il punto di incontro su di una serie di modelli di comportamento da seguire in materia di sicurezza informatica a livello internazionale. Un tale risultato costituisce un delicato compromesso raggiunto dopo intensi dibattiti e malgrado la posizione critica assunta dall'Iran. Quest'ultimo, infatti, pur non impedendo che il documento venisse approvato per consensus, ha ritenuto di "dissociarsi" perché a suo avviso il rapporto include "unacceptable content"[24].

---

[17] Cfr. J. A. Lewis, "Toward a More Coercive Cyber Strategy Remarks to U.S. Cyber Command Legal Conference", 4 marzo 2021, disponibile al link https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[18] Si vedano al riguardo i puntuali rilievi di Michael Schmitt in "Germany's Positions on International Law in Cyberspace Part II", disponibile al link https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/.

[19] Cfr. The Federal Government cit., p. 16.

[20] *Ibid.*

[21] Cfr. UN General Assembly. Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, A/AC.290/2021/CRP.2, 10 marzo 2021.

[22] Il GGE è composto da venticinque membri ed è stato creato dall'Assemblea Generale nel 2004 (cfr. Assemblea generale ONU, A/RES/58/32, 8 dicembre 2003).

[23] Cfr. Assemblea Generale, UN Doc. A/RES/73/266, 2 gennaio 2019, par. 1-3. L'ultimo lavoro del GGE nel 2017 è terminato con un fallimento giacché, in assenza di un accordo tra gli Stati, non ha potuto adottare alcuna relazione.

[24] Cfr. http://webtv.un.org/search/10th-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-third-substantive-session-8-12-march-2021/6239811306001/?term=10th%20meeting%20-%20Open-

ISSN 2279-7238

L'aspetto più significativo del rapporto è costituito dal fatto che recepisce le conclusioni raggiunte dal GGE nel 2015 sui seguenti temi: minacce esistenti ed emergenti; norme, regole e principi; *confidence-building measures*; *capacity building*; e l'applicazione del diritto internazionale, in particolare la Carta ONU, nel cyberspazio[25]. L'accettazione del framework normativo del 2015 è di particolare rilievo perché, come è stato osservato, fornisce una "basis for collective response to actions that violate them"[26]. Tra le questioni più innovative affrontate dal rapporto si segnalano, tra l'altro, i riferimenti alla protezione di specifiche infrastrutture critiche quali le apparecchiature mediche e l'affermazione che gli Stati cercheranno di garantire la disponibilità generale e l'integrità di Internet[27].

ended%20Working%20Group%20on%20Developments%20in%20the%20Field%20of%20Information%20and%20Telecommunications%20in%20the%20Context%20of%20International%20Security,%20Third%20Substantive%20session%20(8-12%20March%202021)&sort=date. V. in particolare il minuto 1:15. La posizione iraniana, senza precedenti nel contesto onusiano, ha richiesto la soppressione, ad ogni capoverso del rapporto, della consueta espressione "States agreed".

[25] Cfr. A/AC.290/2021/CRP.2, par. 7.

[26] Cfr. https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.

[27] Cfr. A/AC.290/2021/CRP.2, par. 18.

ISSN 2279-7238