IL CASO *WANNACRY*: IL FENOMENO DEI *CYBER ATTACKS* NEL CONTESTO DELLA RESPONSABILITÀ INTERNAZIONALE DEGLI STATI

DANIELE MANDRIOLI

1. Il 12 maggio 2017 i sistemi informatici di moltissime imprese private e di apparati statali sono stati vittime di un poderoso *cyber attack*[1], avvenuto mediante la proliferazione di un *malware*, conosciuto come *WannaCry*, all'interno delle reti informatiche[2]. L'attacco si è perpetuato per la durata di tre giorni, durante i quali ha raggiunto dimensioni globali, colpendo più di trecentomila computer dislocati nei territori di centocinquanta Stati[3].

L'estensione e la rilevanza dei danni causati dalla diffusione di *WannaCry* manifestano la pericolosità che caratterizza la commissione degli attacchi informatici nel periodo storico contemporaneo[4]. Alla luce di ciò, il

[1] Con il termine *cyber attack* ci si riferisce a: «any action taken to undermine the functions of a computer network for a political or national security purpose», A. HATHAWAY, R. CROOTOF, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 821.

[2] Per una dettagliata descrizione dei fatti si rimanda a R. BRANDOM, *UK hospitals hit with massive ransomware attack*, in *The Verge*, 12 maggio 2017; N. PERLOTH, D. SANGER, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, in *The New York Times*, 12 maggio 2017; J. WONG, O. SOLON, *Massive ransomware cyber-attack hits nearly 100 countries around the world*, in *The Guardian*, 12 maggio 2017.

[3] Sul funzionamento del *malware WannaCry*, sulle modalità dell'attacco e sulle sue conseguenze, si veda Q. CHEN; R. BRIDGES, *Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware*, 2017, in *16th IEEE International Conference on Machine Learning and Applications* (ICMLA), 2017, 454 ss.

[4] Con riferimento al fenomeno dei *cyber attacks*, è opportuno ricordare che, ben prima del verificarsi dell'attacco *WannaCry*, si era già assistito a tentativi di regolamentazione della loro disciplina in ambito internazionalistico. Un importante sforzo è stato compiuto dalla NATO, in seguito agli attacchi cibernetici ai danni dell'Estonia nel 2007, tramite l'istituzione di un organo interno, dedicato esclusivamente all'analisi del fenomeno degli attacchi cibernetici: il *Centro di Eccellenza della NATO di Tallinn*. All'esito della ricerca condotta dagli esperti NATO, nel 2013, è stato pubblicato il *Tallinn Manual*, che ambisce a essere il prodotto degli sforzi di autorevoli esperti in materia. Inoltre, la cooperazione internazionale

presente lavoro si propone di inquadrare il fenomeno dei *cyber attacks* nell'ambito della responsabilità internazionale degli Stati. Il proliferare di questa tipologia di attacchi impone la necessità di comprendere se e quando uno Stato possa essere ritenuto responsabile della condotta in esame, e quali siano le conseguenze connesse a tale responsabilità.

Partendo dall'osservazione dei fatti caratterizzanti l'attacco *WannaCry*, si intende inquadrare gli stessi all'interno dello schema normativo dettato dal *Progetto di articoli sulla responsabilità per illeciti internazionali degli Stati*[5], elaborato dalla Commissione di diritto internazionale. L'analisi del caso in esame permette ulteriori spunti di riflessione inerenti alla questione giuridica della sussistenza e dell'eventuale violazione di norme internazionali volte a prevenire e reprimere vicende informatiche dannose. Il tema della cosiddetta *cyber-due diligence* viene analizzato nel presente lavoro, in modo da offrire un panorama circa le principali questioni concernenti l'analisi del fenomeno degli attacchi informatici nel contesto della responsabilità internazionale degli Stati.

2. Come brevemente accennato, durante il mese di maggio del 2017, un insidioso attacco informatico, condotto attraverso la produzione e la diffusione del *malware Wannacry*, ha colpito un elevato numero di sistemi informatici dislocati in diversi Stati[6]. L'attacco in questione è stato definito dagli esperti come un'offensiva informatica *ransomware*, consistente nella propagazione di un virus in grado di "prendere in ostaggio" i computer

---

con riferimento al *cyber context* si è concretizzata anche a livello regionale. Nel 2004, l'UE, per mezzo del regolamento (CE) n. 460/2000, del 29 febbraio 2000, ha istituito la European Network and Information Security Agency (ENISA), un centro di competenze in materia di sicurezza informatica. Essa aiuta l'Unione e i Paesi membri a prevenire, rilevare e reagire rispetto ai problemi di sicurezza informatica. Gli Stati del continente asiatico hanno affrontato il delicato tema mediante il *Joint Ministerial Statement* of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation del 13 settembre 2013. E ancora, si leggano le risoluzioni dell'Assemblea generale ONU, *Combating the criminal misuse of information technologies*, UN Doc. A/RES/55/63 del 22 gennaio 2001; *Combating the criminal misuse of information technologies*, UN Doc. A/RES/56/121 del 23 dicembre 2002; *Creation of a global culture of cybersecurity*, UN Doc. A/RES/57/239 del 31 gennaio 2003; *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, UN Doc. A/RES/58/199 del 30 gennaio 2004; *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UN Doc. A/RES/64/211 del 17 marzo 2010. Inoltre, l'ONU ha istituito un gruppo di esperti sul tema: *the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of the United Nations* (UN GGE).

[5] Commissione di diritto internazionale, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, by James Crawford*, *Special Rapporteur*, UN doc. A/CN.4/SER.A/2001/Add. 1 (Part 2), 26.

[6] V. *supra*, nota 3.

infettati[7]. L'utente del dispositivo colpito non può avere accesso alle informazioni in esso contenute, né può servirsi dei programmi installati al suo interno. Il sistema di blocco dei computer causato dagli attacchi *ramsomware* è finalizzato ad un pagamento di un riscatto in denaro. Nel caso in questione, la transazione imposta da *WannaCry* è consistita in una richiesta economica da soddisfare mediante un pagamento in *bitcoin*, la più nota cripto-valuta circolante nel *web*[8].

Una volta colpiti importanti *server* internazionali[9], *WannaCry* si è propagato servendosi del funzionamento di un programma informatico in esso contenuto: *Eternal Blue*[10]. In altre parole, all'interno di *WannaCry*, oltre alla componente *ransomware*, era presente anche un virus in grado di agevolare la proliferazione dell'attacco ai danni degli *hardware* sui quali era installato il sistema operativo *Microsoft Windows*. L'utilizzazione di *Eternal Blue* ha permesso ai creatori di *WannaCry* di "infettare" molteplici macchine in un lasso di tempo estremamente ridotto, realizzando quella che può essere effettivamente definita come una "epidemia informatica globale".

In ragione delle conseguenze che l'attacco in esame ha cagionato, *WannaCry* è stato considerato il *cyber attack* più esteso mai lanciato fino ad oggi[11]. Esso, oltre a danneggiare economicamente un elevato numero di imprese private, ha bersagliato anche diversi organi statali, a cui erano affidate importanti funzioni. In particolar modo, *WannaCry* ha paralizzato

---

[7] Con il termine *ransomware*, si intende: «a class of self-propagating malware that uses encryption to hold victim's data ransom and has emerged as a dominant worldwide threat, crippling personal, industrial, and governmental networked resources», Q. CHEN; R. BRIDGES, *op. cit.*, 454.

[8] Il *bitcoin* è un programma informatico in grado di connettere via internet una pluralità utenti e, mediante tali connessioni, di instaurare un rapporto negoziale fondato su uno specifico valore economico-monetario. O. BJERG, *How is Bitcoin Money?*, in *Culture & Society*, 2015, 55, lo definisce: «a virtual network that allows users to transfer digital coins to each other. Each bitcoin consists of a unique chain of digital signatures that is stored in a digital wallet installed on the user's computer. The wallet generates keys used for sending and receiving coins. A transfer of bitcoins is made as the current owner of the coin uses a private digital key to approve of the addition of the recipient's key to a string of previous transactions. The coin is then transferred and now appears in the recipient's wallet with a recorded history of transactions, including the one just recently completed».

[9] La diffusione di *WannaCry* è avvenuta principalmente mediante il ricorso alla tecnica offensiva del *pishing*. Si tratta di una tipologia di truffa in rete con la quale il creatore cerca di ingannare le vittime convincendole a fornire informazioni personali o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. Il malintenzionato effettua un invio plurimo di messaggi di posta elettronica che imitano messaggi di fornitori di servizi.

[10] Tale programma è definito dagli esperti come un *exploit* del protocollo SMB (*Server Message Block*) di *Windows*. Con tale espressione, si intende un programma informatico in grado di conoscere e sfruttare le lacune e i difetti di un dato protocollo. Nel caso in questione, il *malware Eternal Blue* è stato ideato con la specifica finalità di sfruttare i limiti del protocollo SMB di *Microsoft*, ovvero un protocollo utilizzato per condividere *file*s, stampanti, porte seriali e comunicazioni di varia natura tra diversi nodi di una rete.

[11] V. *supra*, nota 3.

per alcuni giorni il funzionamento del sistema sanitario del Regno Unito, causando gravissime conseguenze[12].

Secondo quanto affermato dal Lord Ahmad of Wimbledon, il Ministro degli affari esteri britannico ai tempi dell'attacco, le condotte di realizzazione e diffusione in rete del virus sarebbero state opera di un gruppo di *hacker* di nazionalità nord coreana: Lazarus[13]. Tali accuse si fondano su un'attenta comparazione dei codici solitamente utilizzati dal gruppo di *hacker* per i suoi attacchi e quelli costitutivi di *WannaCry*. Il gruppo avrebbe personalmente creato la componente *ransomware* del *malware*, a cui poi avrebbe aggiunto il preesistente programma *Eternal Blue*. Quest'ultimo, secondo il parere degli esperti, era stato già precedentemente sviluppato dall'NSA americana, e diffuso illegalmente durante i primi mesi del 2017 da un'altra compagine di *hacker*, nota come The Shadow Brokers[14].

3. Una volta esposti i fatti dell'attacco informatico in esame, ci si propone ora di inquadrare lo stesso all'interno della disciplina della responsabilità internazionale degli Stati. Com'è noto, nel diritto internazionale pubblico, il Progetto di articoli sulla responsabilità per illeciti internazionali degli Stati (d'ora in avanti, il Progetto) si occupa di tale questione e ambisce ad esprimere la codificazione del diritto consuetudinario del *corpus* di norme secondarie in tema di illeciti[15].

---

[12] Si riporta quanto raccontato da Brad Smith, presidente dell'ufficio legale di *Microsoft*, in un discorso pubblico del 10 novembre 2017: «In May, the nation state-sponsored WannaCry ransomware attack impacted more than 200,000 computers in more than 150 countries and showed the world the broad damage "invisible" cyber weapons can inflict. This didn't just cause damage to machines. As the United Kingdom's National Audit Office concluded just last week, WannaCry's impact forced the National Health Service to divert ambulances and cancel over 19,000 appointments for people scheduled to see a physician or have a surgical procedure». Per una narrazione giornalistica concernente le conseguenze degli attacchi di *WannaCry*, v. R. BRANDOM, *op. cit*. Anche l'Italia è stata vittima di *WannaCry*, il quale ha colpito alcuni computer dell'Università statale Bicocca di Milano.

[13] Secondo una sua dichiarazione ufficiale del 19 dicembre 2017: «The UK's National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign – one of the most significant to hit the UK in terms of scale and disruption». Anche il Dipartimento di difesa degli Stati Uniti ha condiviso la denuncia portata avanti dal Regno Unito. Lazarus è uno dei più noti e pericolosi tra gruppi di *hacker* di questo decennio e, secondo alcuni esperti, avrebbe partecipato alla commissione dell'attacco informatico ai danni della Sony, nel 2014. Inoltre, il gruppo di *hacker* sembra essere coinvolto anche nel *cyber attack* del 2016 contro la banca nazionale del Bangladesh.

[14] Sul tema della sottrazione ai danni dell'NSA di *Eternal Blue* e della sua utilizzazione da parte del gruppo Lazarus, v. E. ATSU, *Understanding the Wannacry Ransomware*, in *Linked In*, 20 maggio 2017.

[15] La Corte internazionale di giustizia ha analizzato in diverse pronuncie la rilevanza consuetudinaria del Progetto del 2001. Cfr., *ex multis*, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v. Serbia and Montenegro*), sentenza del 26 febbraio 2007, paragrafi 173-174; *Pulp Mills on the River*

Come evidenziato dalla dottrina maggioritaria[16], gli articoli del Progetto risultano essere la base normativa sulla quale si fonda l'analisi del fenomeno dei *cyber attacks* nel prisma della disciplina della responsabilità internazionale degli Stati. Ciò premesso, in questa sede si vuole analizzare se le condotte di produzione e diffusione del *malware WannaCry* possano integrare un illecito internazionale[17].

La commissione di un *cyber attack* risulta illecita se implica la violazione di un obbligo di diritto internazionale[18]. Conseguentemente, diviene necessario comprendere se esista all'interno dell'ordinamento una norma, di natura consuetudinaria o pattizia, consistente in uno specifico divieto in capo agli Stati di commettere un *cyber attack*, la cui violazione configurerebbe la presenza dell'elemento oggettivo della responsabilità internazionale. In relazione a tale quesito, occorre osservare che una disposizione del genere non si è ancora affermata[19].

Tale assenza impone alcune riflessioni. Secondo il principio espresso dalla Corte permanente internazionale di giustizia nel caso *Lotus*, «restrictions upon the indipendence of States cannot be presumed»[20]. Per

---

Uruguay (*Argentina v. Uruguay*), sentenza del 20 aprile 2010, par. 152. L'attività di codificazione effettuata dagli articoli del Progetto viene maggiormente analizzata in Assemblea generale, *Responsibility of States for Internationally Wrongful Acts – Compilation of Decisions of International Courts, Tribunal and other Bodies*, *Report of the Secretary General*, UN Doc. A/65/76, 2010.

[16] Si leggano *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge, 2017, 80: «the customary international law of State responsibility undeniably extends to cyber activities»; nonché M. ROSCINI, *Cyber Operations and Use of Force,* London, 2014, 34; K. MACAK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict & Security Law*, 2016, 406.

[17] Si riporta quanto codificato dall'art. 2 del Progetto del 2001: «There is an internationally wrongful act of a State when conduct consisting of an action or omission: (*a*) is attributable to the State under international law; and (*b*) constitutes a breach of an international obligation of the State». La necessaria contemporanea sussistenza degli elementi oggettivo e soggettivo al fine dell'applicazione della disciplina della responsabilità internazionale è stata ribadita anche dalla Corte internazionale di giustizia in molteplici sentenze, tra le quali v. le sentenze del 24 maggio 1980, *United States Diplomatic and Consular Staff in Tehran* (*United States of America v. Iran*), par. 56; del 27 giugno 1986, *Military and Puramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America). Merits*, par. 226; e del del 25 settembre 1997, *Gabcikovo-Nagymaros Project* (*Hungary v. Slovakia*), par. 78.

[18] L'art. 12 del Progetto specifica chiaramente che, per violazione dell'obbligo internazionale, debba intendersi: «an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character».

[19] L'assenza di un *corpus* di norme consuetudinarie specificamente dedicato alla regolamentazione del contesto cibernetico è affermata e analizzata da G.M. RUOTOLO, *Internet (diritto internazionale)*, in *Enciclopedia del diritto*, *Annali*, VII, 2014, 549.

[20] Sentenza del 7 settembre 1927, *The Case of the S.S. "Lotus"* par. 18 s.

alcuni studiosi[21], ciò impone una presunzione di legittimità delle condotte non esplicitamente vietate da alcuna norma di diritto internazionale. Tuttavia, queste considerazioni non escludono necessariamente l'illiceità della commissione di un attacco informatico laddove operino delle disposizioni generali dell'ordinamento che, pur non riguardando specificatamente la fattispecie in esame, possano essere analogicamente applicabili al caso concreto. Ogniqualvolta la condotta esaminata configuri la violazione di un divieto generalmente prescritto dal diritto internazionale, si potrà affermare la sussistenza dell'elemento oggettivo della responsabilità internazionale, anche in assenza di una norma di esplicita condanna degli attacchi cibernetici[22].

Con riferimento a tale tematica, merita di essere attentamente analizzato l'eventuale contrasto dell'attacco *WannaCry* rispetto al principio di non intervento[23]. La Corte internazionale di giustizia, nel caso *Nicaragua v. United States*[24], ha affermato l'esistenza di una prescrizione di origine consuetudinaria consistente nel divieto in capo agli Stati di intervenire, direttamente o meno, negli affari interni o esterni di altri Stati[25]. Esso è un corollario del principio della sovranità territoriale degli Stati, elemento cardine della struttura della Comunità internazionale, il quale comporta

[21] L'analisi del caso *Lotus* ha stimolato la dottrina ad affrontare alcune delicate questioni di struttura del sistema dell'ordinamento giuridico internazionale. In particolar modo, è fortemente connesso all'analisi del caso la problematica questione circa la natura positiva o meno del sistema di diritto internazionale pubblico. Il tema è analiticamente affrontato in O. SPIERMANN Lotus *and the Double Structure of International Legal Argument*, in P. SANDS, L BOISSON DE CHAZOURNES (eds.), *International Law, the International Court of Justice and Nuclear Weapons*, London, 1999, 131-151.

[22] La tematica inerente al ricorso all'applicazione analogica del sistema normativo del diritto internazionale, al fine di colmare l'assenza di disposizioni specifiche nell'ambito del *cyberspace*, è analizzata da D. HOLLIS, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, in J.D. OHLIN, K. GOVERN, C. FINKELSTEIN (eds.), *Cyber War, Law and Ethics for Virtual Conflicts*, Oxford, 2015, 129-175. Sul tema, si riporta anche quanto affermato da K. MACAK, *International Law and Practice, From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, in *Leiden Journal of International Law*, 2017, 883: «The absence of a cyber-specific system of rules of international law does not mean that there are no legal rules that would apply to cyber activities».

[23] La sussistenza del principio di non intervento viene fortemente richiamata dalla dottrina anche nello specifico tema dell'analisi delle condotte cibernetiche. Sul tema, v. I. DETTER, *The Law of War, Second Edition*, London, 2000, 72; M. ROSCINI, *op. cit*., 46; N. TSAGOURIAS, R. BUCHAN, *International Law and Cyber Space*, Cheltenham, 2015, 65.

[24] Nella sentenza *Nicaragua v. United States*, paragrafi 202-209, la Corte analizza dettagliatamente la natura giuridica del principio in esame.

[25] Si legga quanto affermato dalla Corte nel caso *Nicaragua v. United States*, par. 205: «The principle forbids al1 States or groups of States to intervene directly or indirectly in internal or external affairs of other States». L'esistenza del principio di non intervento all'interno dell'ordinamento internazionale è confermata dall'art. 8 della Convenzione di Montevideo sui diritti e obblighi degli Stati, 1933: «No State has the right to intervene in the internal or external affairs of another».

«[the] right of every sovereign State to conduct its affairs without outside interference»[26].

Il tema dell'individuazione dei confini applicativi del principio di non intervento è stato oggetto di attenta analisi da parte della dottrina[27] e della giurisprudenza[28], che concordano nel non interpretare estensivamente tale divieto; pressanti azioni economiche o diplomatiche, ad esempio, realizzano tipici interventi che il diritto internazionale tollera e che, conseguentemente, non costituiscono di per sé una violazione della disposizione in esame. Secondo l'opinione prevalente, un'ingerenza risulta proibita solo quando assuma connotati tali da limitare un altro Stato nell'esercizio libero dei propri affari interni o esterni. In altre parole, un intervento, per poter essere lecito, non deve essere *coercitivo*[29]. Lo Stato che subisce un'ingerenza deve rimanere in grado di esercitare liberamente i propri poteri sui piani politico, economico, sociale, culturale e di politica estera[30]; in caso contrario, tale intervento assumerà i connotati della violazione di un obbligo internazionale.

Facendo leva sul concetto di *coercion* richiamato dalla Corte internazionale di giustizia, l'analisi degli attacchi commessi mediante l'utilizzazione e la diffusione del *malware WannaCry* evidenzia la loro potenziale illegittimità secondo il diritto internazionale. Questo attacco informatico, infatti, oltre ad aver danneggiato economicamente diverse imprese, ha direttamente colpito alcuni organi statali, precludendoli la possibilità di esercitare liberamente le funzioni a loro affidate. Nonostante la scarsità di informazioni certe sulle conseguenze di questi attacchi renda difficile ravvisare con sicurezza una violazione del principio di non intervento, ciò non può essere escluso[31]. Inoltre, è interessante notare come queste intrusioni possano

---

[26] Caso *Nicaragua v. United States*, par. 202. Sul tema, si veda in generale R. SAPIENZA, *Il principio di non intervento negli affari interni*, Milano, 1990; A. CASSESE, *International Law*, London, 2005, 98-100; M. KOHEN, *The Principle of Non-Intervention 25 Years after the Nicaragua Judgment,* in *Leiden Journal of International Law*, 2012.

[27] Oltre ai richiami alla giurisprudenza internazionale ed alle risoluzioni delle organizzazioni internazionali, autorevole dottrina si è occupata del principio di non intervento e dei suoi confini di applicazione. Secondo L.F. L. OPPENHEIM, *International Law*, London, 1992, 432: «the interference must be forcible or dictatorial depriving the state of control over the matter in question».

[28] A conferma di ciò, si legga quanto disposto dalla Corte internazionale di giustizia in *Nicaragua v. United States*, par. 205.

[29] *Ibidem*, par. 205: «The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention».

[30] *Ibidem*: «to choose freely its political, economic, social, cultural system and the formulation of foreign policy».

[31] Con riferimento ad un ulteriore e successivo *cyber attack*, l'attacco *Not-Petya* del giugno 2017, il quale presenta particolari analogie rispetto al caso *WannaCry*, secondo M. SCHMITT, L. BILLER, *The Not-Petya Cyber Operation as a Case Study of International Law*, in *EJIL Talk!*, 2017, reperibile *online*: «NotPetya may have affected the domaine réservé of one or more States; additional information would be useful in this regard. Although ransomware is a paradigmatic means of cyber coercion, the paucity of evidence as to the motivations underlying NotPetya make it difficult to label the operation coercive».

costituire manovre coercitive a danno degli Stati colpiti non solo per quanto riguarda le conseguenze che hanno determinato, ma anche e soprattutto per quanto concerne le modalità con le quali esse sono state condotte. Come specificato precedentemente, l'attacco *WannaCry* si è sostanziato in una tipica condotta di estorsione. Ne deriva che la condotta in esame risulta per sua natura coercitiva. Infatti, essa pone le vittime nella condizione di dover pagare un riscatto al fine di utilizzare nuovamente la macchina infettata. Risulta altrettanto intuitivo che, nell'eventualità in cui l'attacco colpisca organi statali, come nel caso in questione, tale coercizione viola il principio di non intervento, in conformità con quanto ribadito da dottrina e giurisprudenza. I fatti di maggio 2017 evidenziano con chiarezza la potenzialità degli strumenti informatici di realizzare pericolose intromissioni e ingerenze pregiudizievoli allo svolgimento delle funzioni degli Stati colpiti[32]. L'affidamento che gli Stati ripongono negli strumenti informatici per lo svolgimento di fondamentali funzioni interne ed esterne accresce il rischio del verificarsi di tali intrusioni nella gestione dei propri affari mediante *cyber attack*[33]. L'ottemperanza al principio di non intervento diviene il primo e fondamentale limite imposto dall'ordinamento in tema di realizzazione di azioni cibernetiche[34] e la sua inottemperanza concretizza l'elemento oggettivo della responsabilità internazionale[35].

4. L'inquadramento del caso *WannaCry* nel contesto della responsabilità internazionale degli Stati impone un'analisi che non si esaurisca nella dimostrazione della contrarietà della condotta in esame rispetto alle norme primarie dell'ordinamento giuridico internazionale, poiché dev'essere necessariamente affrontata la delicata questione dell'attribuzione della condotta illecita ad uno Stato[36].

---

[32] Sul tema, si veda quanto scritto da M. SCHMITT, *Wired Warfare: Computer Network Attack and the Jus in Bello*, in *International Law Studies*, 2002, 188.

[33] V. l'attenta analisi di S. HERZOG, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, in *Journal of Strategic Security*, 2011, 50.

[34] Si veda in questo senso quanto scritto da R. BUCHAM, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in *Journal of Conflict & Security Law*, 2012, 212-227.

[35] Si riporta quanto affermato in G.M. RUOTOLO, *Internet-ional Law*, Bari, 2012, 143: «gli attacchi informatici che non raggiungono una tale soglia di aggressività – e quindi non comportano la distruzione di beni e la Perdita di vite umane – riteniamo siano comunque vietati dal diritto internazionale potendo rappresentare, in alcuni casi limite, forme di minaccia dell'uso della forza e in altri casi, meno qualificati, comunque una violazione del principio di non ingerenza negli affari interni di uno Stato».

[36] Come noto, l'art. 2 Progetto del 2001 dispone che l'illiceità di un atto si scompone in due elementi, oggettivo e soggettivo, la contemporanea presenza dei quali comporta l'applicazione della disciplina della responsabilità internazionale. Tale disposizione codifica una norma consuetudinaria, come storicamente espresso già dalla Corte permanente internazionale di giustizia, nella sentenza del 14 giugno 1938, *Phosphates in Marocco*, p. 10, e ribadito dalla Corte internazionale di giustizia nella sentenza relativa al caso *United States Diplomatic and Consular Staff in Tehran*, par. 56; 90. Con diretto riferimento alla materia

La disciplina dell'elemento soggettivo dell'illecito segue quanto codificato negli articoli 4-11 del Progetto del 2001[37]. Com'è noto, tale analisi si sostanzia principalmente in una triplice operazione giuridica[38]. In primo luogo, si deve valutare se la condotta illecita possa essere attribuita ad un organo *de iure* dello Stato[39]. In secondo luogo, lo Stato è ritenuto autore dell'illecito anche laddove la violazione sia commessa da uno o più individui, il cui rapporto con lo Stato si ravvisa esclusivamente a livello organico *de facto*[40]. Infine, laddove l'illecito sia stato commesso da un singolo o da un gruppo di persone esterne rispetto alla struttura organizzativa dello Stato, la responsabilità di quest'ultimo può comunque essere affermata nel caso in cui il privato abbia agito sotto le istruzioni, la direzione o il controllo dello Stato stesso[41].

Come già evidenziato, secondo la valutazione degli esperti e secondo le accuse degli Stati vittime, l'attacco *WannaCry* sarebbe stato lanciato dal

---

informatica, gli autori del *Tallinn Manual 2.0* concordano nel ritenere che la disposizione contenuta nell'art. 2 del Progetto si applichi totalmente anche al contesto cibernetico, come si evidenzia nella *rule* 14: «A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation».

[37] La disciplina contenuta nel Progetto del 2001 sul tema dell'elemento soggettivo riprende fedelmente la prassi internazionalistica precedentemente consolidatasi, che trova origine in quanto storicamente affermato dalla Corte internazionale di giustizia nella sentenza resa nel caso *United States Diplomatic and Consular Staff in Tehran*, paragrafi 56-61.

[38] Gli articoli del Progetto in materia di attribuzione evidenziano ulteriori modalità di individuazione dell'elemento soggettivo. L'art. 5 ravvisa l'individuazione dell'elemento soggettivo laddove la condotta illecita sia stata commessa da una struttura para-statale; l'art. 10 attribuisce la condotta allo Stato laddove questa sia stata commessa da gruppi insurrezionali i quali successivamente acquisiscono una soggettività internazionale; l'art. 11 individua la presenza dell'elemento soggettivo laddove la condotta, anche se realizzata da individui privati, venga approvata e fatta come propria dallo Stato. Nel presente lavoro, l'attenzione si incentra esclusivamente sul sistema tripartito di analisi attributiva, così come delineato dalla Corte internazionale di giustizia nella sentenza resa nel caso *Bosnia Herzegovina v. Serbia e Montenegro*, par. 384. Le altre modalità di attribuzione, per quanto rilevanti a livello teorico, non sono particolarmente problematiche in materia cibernetica.

[39] La possibilità di attribuire la condotta ad un organo *de iure* è sancita dall'art. 4, par .1, del Progetto: «The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State».

[40] La responsabilità internazionale dello Stato derivante dalla commissione di una condotta illecita da parte di un organo *de facto* è evidenziata dalla lettura dell'art. 4, par. 2, del Progetto: «An organ includes any person or entity which has that status in accordance with the internal law of the State». Il termine "*includes*" chiarisce come il diritto internazionale non limiti la propria considerazione del concetto di organo esclusivamente con riferimento a quello disciplinato dal diritto interno di uno Stato, ma considera questa ipotesi come una fattispecie da inserire all'interno di un insieme maggiormente esteso, il quale ricomprende anche strutture statali costitutive dell'organizzazione statale, pur senza essere definite e regolate dalla legge nazionale.

[41] Il criterio dell'attribuzione allo Stato delle condotte commesse da individui privati è codificato nell'art. 8 del Progetto.

gruppo di *hacker* Lazarus, il quale avrebbe agito supportato dallo Stato della Corea del Nord[42]. Pur tralasciando in questa sede la questione circa l'evidente difficoltà probatoria in materia di attribuzione dei *cyber attacks* ai loro reali autori[43], ipotizzando quindi che le accuse rivolte contro Lazarus siano fondate, la possibilità di attribuire la condotta illecita ad uno Stato rimane estremamente controversa. Infatti, anche laddove si riuscisse a dimostrare che l'attacco *WannaCry* sia stato effettivamente commesso dal gruppo Lazarus, quest'ultimo non potrebbe essere definito un organo *de iure* di alcuno Stato[44], e quindi non risulterebbe operativo il criterio primario di attribuzione dell'illecito codificato dall'art. 4, par. 1, del Progetto.

Conseguentemente, occorre esplorare la possibilità di applicare al caso concreto la disciplina dell'organo *de facto* e, residualmente, il meccanismo di attribuzione allo Stato della condotta dei privati sottostanti al suo controllo[45]. Per quanto concerne la prima opzione, un individuo o un gruppo di individui possono essere ritenuti un organo *de facto* soltanto qualora essi agiscano in completa dipendenza di uno Stato[46]. Il parametro di completa dipendenza viene essenzialmente definito come: «proof of a particularly great degree of State control over them»[47]. Osservando ora il presunto legame intercorrente tra il gruppo Lazarus e la Corea del Nord, si deve constatare come la dimostrazione dell'esistenza di tale relazione risulti essere parti-

[42] V. *supra*, nota 14.

[43] L'odierna struttura della rete internet, costituita da un sistema informatico che consapevolmente si fonda sui connotati di anonimità, incertezza e volatilità delle comunicazioni, risulta essere l'origine dei problemi attributivi che caratterizzano le *cyber activities*. Le relazioni informatico-digitali si differenziano da tutte le altre per la loro tipica inafferrabilità. La questione probatoria degli attacchi informatici è attentamente approfondita da A. BUFALINI, *Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico*, in A. LANCIOTTI, A. TANZI (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2012, 430 ss.; N. TSAGOURIAS, *Cyber attacks, self-defence and the problem of attribution*, in *Journal of Conflict & Security Law*, 2012, 229-244; T. RID; R. BUCHANAN, *Attributing Cyber Attacks*, in *The Journal of Strategic Studies*, 2015, 5-37; M. ROSCINI, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in *Texas International Law Journal*, 2015.

[44] Si ricorda in questa sede che il commentario dell'art. 4 del Progetto, al par. 6, definisce il termine '*State organ*' come: «all the individual or collective entities which make up the organization of the State and act on its behalf». Il gruppo di *hacker* accusato dell'attacco *WannaCry* non ha alcun rapporto formale con uno Stato. Conseguentemente, l'attacco informatico qui analizzato non è riconducibile ad alcuno Stato *ex* art. 4 del Progetto.

[45] Tale ordine nel ricorso ai criteri di individuazione dell'elemento soggettivo, come ricordato precedentemente, si fonda sul sistema tripartito di analisi attributiva delineato dalla Corte internazionale di giustizia nella sentenza resa nel caso *Bosnia Herzegovina v. Serbia e Montenegro*, par. 384.

[46] *Ibidem*, par. 392: «persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in "complete dependence" on the State, of which they are ultimately merely the instrument».

[47] *Ibidem*, par. 392.

colarmente problematica. Detta difficoltà non deriva esclusivamente dall'elevato livello di dipendenza richiesto dal diritto internazionale al fine di individuare una relazione fattuale tra gli individui agenti e lo Stato, ma anche e soprattutto dalla complessità della fase probatoria che caratterizza le condotte cibernetiche[48]. Sulla base delle informazioni rese note sul caso *WannaCry*, non sembra ravvisabile la presenza di un legame di completa dipendenza tra l'organizzazione privata Lazarus ed alcuno Stato.

Infine, in via residuale e sussidiaria, l'elemento soggettivo della responsabilità derivante dall'attacco *WannaCry* potrebbe essere individuato utilizzando il criterio di attribuzione codificato dall'art. 8 del Progetto[49]. Questa modalità di attribuzione si fonda su una relazione fattuale intercorrente tra gli attori privati e lo Stato, per mezzo della quale «a State may, either by specific directions or by exercising *control* over a group, in effect assume responsibility for their conduct»[50]. Com'è noto, l'analisi del concetto di controllo è stata affrontata dalla Corte internazionale di giustizia[51], che ha esplicitamente evidenziato come l'applicazione del criterio di attribuzione codificato dall'art. 8 necessiti la dimostrazione della sussistenza di un livello di controllo tale da poter essere definito *effettivo*[52]. La teoria del controllo effettivo richiede che non venga semplicemente dimostrata la sussistenza di una relazione di coordinamento generale delle condotte dei privati da parte dello Stato, ma anche che tale controllo sia

[48] A conferma di tale considerazione, v. D. HOLLIS, *An e-SOS for Cyberspace*, in *Harvard International Law Journal*, 2011, 378: «Current information technology makes it difficult to identify the actual server from which an attack (or exploit) originates, let alone its perpetrators. And this is not a transient problem - the very architecture of the Internet enables hackers to maintain anonymity if they so desire».

[49] L'applicazione di questo residuale criterio di attribuzione nell'ambito delle *cyber activities* è stata oggetto di importanti analisi da parte della dottrina. V. la *rule* 17 del *Tallinn Manual 2.0*, secondo cui: «cyber operations conducted by a non-State actor are attributable to a State when engaged in pursuant to its instructions or under its direction or control»; nonché S. SHACKELFORD, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, in *Conference on Cyber Conflict Proceedings*, 2010; C. ALLAN, *Attribution issues in Cyberspace*, in *Chicago-Kent Journal of International and Comparative Law*, 2013; T. PAYNE, *Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations*, in *Lewis & Clark Law Review*, 2016, 684-715; K. MACAK, *Decoding Article 8*, cit., 411-412.

[50] Commentario sull'art. 8 del Progetto del 2001, par. 7.

[51] Sentenza d *Bosnia Herzegovina v. Serbia e Montenegro*, paragrafi. 396-412.

[52] L'analisi della disciplina del controllo statale rispetto alle azioni degli attori non organo è stata specificatamente analizzata dalla Corte internazionale di giustizia nella sentenza resa nel caso *Nicaragua v. United States*, par. 115, dove essa ha evidenziato la necessità di dover provare l'*effettività* di tale controllo: «it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed». Nella sentenza *Bosnia Erzegovina v. Serbia e Montenegro*, la Corte ha ribadito quanto affermato precedentemente in materia di controllo, richiedendo la dimostrazione della sua effettività al fine di attribuire la responsabilità della condotta illecita in capo allo Stato.

posto a fondamento delle specifiche azioni che realizzano la condotta illecita commessa da attori privati[53].

Ciò posto, occorre constatare che l'applicazione della teoria del controllo effettivo ai fini dell'attribuzione dei fatti di *WannaCry* conduce a risultati ben poco soddisfacenti. Infatti, l'onere probatorio, già di per sé particolarmente elevato, diviene assai più difficile nel caso di attacchi cibernetici, vista l'anonimità, l'incertezza e la volatilità che caratterizzano le relazioni a livello informatico[54]. Per poter dimostrare che uno Stato abbia svolto un'azione di controllo rispetto alla commissione di tali attacchi, eseguiti attraverso individui non organi, si dovrebbe provare con certezza che esso sia stato diretto promotore di tutte quelle singole condotte che hanno violato il diritto internazionale[55]. Non basterebbe dimostrare la

[53] Ai fini dell'individuazione del parametro del controllo effettivo, non risulta sufficiente dimostrare che lo Stato abbia sostenuto, finanziato e supportato gli attori non organi, se allo stesso momento non si proverà che tale relazione abbia dato forma ad un vero e proprio controllo da parte dello Stato sulle specifiche condotte in esame, in modo tale da evidenziare come questo sia stato *effettivo* rispetto all'illecito che si vuole attribuire allo Stato stesso. Si richiama quanto dichiarato esplicitamente dalla Corte internazionale di giustizia nella sentenza *Nicaragua v. United States*, par. 115. La definizione di controllo effettivo viene analizzata più dettagliatamente dalla stessa Corte nella sentenza *Bosnia Erzegovina v. Serbia e Montenegro*, par. 400: «It must however be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations».

[54] Le problematicità derivanti dall'applicazione de parametro del controllo effettivo rispetto alle condotte cibernetiche sono segnalate da S. SHACKLEFORD, *op. cit*., 201: «Given what has been demonstrated about the extreme technical difficulties of proving the identity of cyber attacks due to the nature of the Web's architecture, such a standard would in essence give a free pass to State sponsors of cyber attacks. (…) Without either new techniques such as the probabilistic tracing project mentioned in Part II, or very unsophisticated hackers, effective control would make State responsibility for cyber attacks virtually a non-starter».

[55] Alcuni autori hanno cercato di individuare delle soluzioni innovative in tema di attacchi cibernetici, volte a garantire una maggiore riconducibilità delle condotte dei privati agli Stati. Merita di essere esposta la teoria incentrata sulla possibilità di applicazione nel contesto cibernetico di un parametro di controllo differente rispetto a quello elaborato dalla Corte internazionale di giustizia, ovvero il parametro del controllo 'globale'. Tale teoria, che si fonda sul parametro di controllo configurato Tribunale penale internazionale per l'ex-Iugoslavia, Appeals Chamber, sentenza del 15 luglio 1999, *Prosecutor v. Tadic*, IT-94-1-A, paragrafi 98 e 145, è sostenuta da S. SHACKLEFORD, *op. cit*., 204: «It should thus be sufficient as matter of international law to prove overall control by a government in a cyber attack, rather than complete control. For example, if the overall control standard were used instead of effective control, it would be possible that Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution. A comprehensive future legal regime could grant Estonia, and other victim nations, adequate reparations for such attacks. But if effective control becomes the dominant paradigm for determining State responsibility for cyber attacks, even a victim State of a worst-case scenario cyber attack may not receive justice».

sussistenza di un legame di cosiddetta "sponsorizzazione"[56] dello Stato rispetto ai privati, ma si dovrebbe ravvisare con certezza il comportamento di direzione e di gestione statale con diretto riferimento all'attacco cibernetico realizzato.

In defintiva, le rilevate incertezza e volatilità in materia probatoria, che caratterizzano tipicamente le relazioni informatico-digitali[57], comportano una difficile applicazione del regime consuetudinario dell'attribuzione dell'illecito così come codificato dagli articoli del Progetto.

5. L'analisi che precede ha evidenziato importanti profili di criticità che rendono problematico l'inquadramento dell'attacco *WannaCry* nel contesto della responsabilità internazionale degli Stati.

Una volta constatata la difficoltà di attribuire tale condotta ad uno Stato, emergono due indesiderate conseguenze di carattere generale. In primo luogo, viene preclusa la possibilità di definire la condotta come illecita ai sensi del diritto internazionale[58]. Inoltre, e conseguentemente, la controversa applicazione della disciplina della responsabilità segnala l'assenza di un valido deterrente all'interno dell'ordinamento volto a fronteggiare il proliferare degli attacchi informatici, le cui conseguenze possono risultare estremamente dannose.

Al fine di individuare dei validi correttivi rispetto all'applicazione inefficace dell'istituto della responsabilità internazionale, occorre ora analizzare l'attacco *WannaCry* con riferimento alla potenziale applicazione degli obblighi di *due diligence* imposti in capo agli Stati dal diritto internazionale. L'eventuale inottemperanza a tali obblighi permetterebbe infatti una censura dei comportamenti statali per lo meno a livello indiretto rispetto alla commissione di un *cyber attack* non attribuibile ad alcuno Stato[59].

---

[56] La presente posizione è fatta propria dai redattori del *Tallin Manual 2.0*, cit., 97. Essi sostengono: «A State's general support for or encouragement of a non-State actor or its cyber operations is insufficient to establish attribution».

[57] Si condivide quanto autorevolmente affermato da J.C. WOLTAG, *Military Cyber Warfare: Cross-Border Computer Network Operations under International Law*, London, 2014, 274: «the major problem in this regard has been shown to be the insufficient technical capacity to track and trace hostile computer network operations to their source systems. As a consequence the legal attributability of the operation is similarly inadequate».

[58] In questa sede, è opportuno riportare quanto chiaramente affermato in J. CRWAFORD, A. PELLET, S. OLLESON, *The Law of International Responsibility*, New York, 2009, 276: «the individual, subject of internal law, cannot breach International law under which he has no obligation. In the same way, the State should not be co-responsible or accomplice to a breach of internal law of the State by an individual».

[59] Si condivide quanto affermato da M. SCHMITT, *In Defence of Due Diligence in Cyber Space*, in *Yale Journal Law Forum*, 2015, 79: «if the territorial state fails to terminate an ongoing non-state cyber operation mounted from its territory against another state, and doing so is practical and reasonable in the circumstances, then the territorial state commits an internationally wrongful act by failing to exercise its obligations under the principle».

Con il termine *due diligence*, nel diritto internazionale si fa riferimento ad un principio generale secondo cui in capo ad ogni Stato è posto un obbligo «not to allow knowingly its territory to be used for acts contrary to the rights of other States»[60]. Tale principio si è consolidato in una prassi costante dalla fine del XIX sec. ad oggi[61].

È largamente condivisa in dottrina la considerazione secondo cui il concetto di diligenza abbia una natura tipicamente flessibile[62]. Da tale aspetto, deriva che le norme di *due diligence* debbano essere considerate come obblighi primari di *condotta* finalizzati a far sì che ogni Stato ottemperi allo standard di diligenza[63] richiesto a seconda della specifica situazione[64]. Il funzionamento di tali norme necessita quindi la strutturazione di parametri di condotta *ad hoc*, differenti a seconda del contesto giuridico-fattuale in esame[65].

---

[60] Questa definizione è data dalla Corte internazionale di giustizia nella sentenza del 9 aprile 1949, *Corfù channel* (*United Kingdom of Great Britain and Northern Ireland v. Albania*), par. 22, e confermata recentemente nella sentenza resa nel caso *Pulp Mills on the River Uruguay*, par. 101.

[61] L'osservazione in chiave storica delle vicende giuridiche in cui si è evidenziata la rilevanza del principio di *due diligence* è contenuta in R. BARNIDGE, *The Due Diligence Principle under International Law*, in *International Community Law Review*, 2006, 81-121; R. PISILLO MAZZESCHI, *Due diligence e responsabilità Internazionale degli Stati*, Milano, 1989. A livello giurisprudenziale, importanti casi hanno affrontato l'analisi del principio di *due diligence*. Tra questi, si ricordano Tribunale arbitrale, lodo del 14 settembre 1872, *Alabama claims of the United States of America against Great Britain*; Tribunale arbitrale, lodo del 26 maggio 1941, *Trail Smelter Case* (*United States v. Canada*); Corte internazionale di giustizia, *Pulp Mills on the River Uruguay*, par. 101.

[62] La caratteristica della flessibilità della *due diligence* è stata storicamente evidenziata dalla dottrina. Si riporta in questa sede quanto affermato da F.V. GARCIA AMADOR, *Second Report on State Responsibility* (UN Doc. A/CN.4/106), 1957, 122: «The learned authorities are in almost unanimous agreement that the rule of due diligence cannot be reduced to a clear and accurate definition which might serve as an objective and automatic standard for deciding, regardless of the circumstances, whether a State was diligent in discharging its duty of vigilance and protection». Ricordando quanto scritto da R. PISILLO MAZZESCHI, *op. cit*., 13-18, il carattere della flessibilità tipico del concetto di diligenza è stato uno dei principali motivi che ha intimorito la dottrina nell'affrontare analiticamente gli obblighi di *due diligence*.

[63] Secondo R. PISILLO MAZZESCHI, *op. cit*., 335, tale standard di diligenza «comprende sia obblighi di prevenzione che di repressione».

[64] È opinione pressoché unanime della dottrina che le norme di *due diligence* debbano essere definite come disposizioni impositive di obblighi di condotta dal carattere flessibile. Tra i vari autori, rimane preminente l'analisi esposta da R. PISILLO MAZZESCHI, *op. cit*., 398-399: «la flessibilità del concetto di *due diligence* consente di diversificare il grado di diligenza in relazione agli standards di comportamento diversi richiesti dal diritto internazionale in ciascuno dei settori in cui tale concetto rileva».

[65] Autorevoli autori, per segnalare la caratteristica della flessibilità, definiscono le norme di *due diligence* come norme relative. Si riporta in questa sede l'attenta osservazione di J. CRAWFORD, *State Responsibility*, Cambridge, 2013, 227: «obligations of due diligence are relative, not absolute».

La dottrina si è recentemente interrogata circa la possibilità di ravvisare la sussistenza di obblighi di *due diligence* nel contesto delle *cyber activities*[66]. Condividendo il ragionamento di esposto da alcuni autori[67], l'assenza di specifiche disposizioni volte a regolamentare le relazioni informatiche non esclude, ma anzi, richiede l'applicazione all'interno di tale settore delle principali e fondamentali disposizioni dell'ordinamento. Alla luce di tale ragionamento, sarebbe quindi possibile applicare il principio di *due diligence*, disposizione di carattere generale ampiamente riconosciuta dal sistema giuridico internazionale[68], anche all'interno di una nuova, ma non autonoma, branca del diritto internazionale, ovvero quella volta a regolamentare il *cyberspace*[69].

Condividendo questo approccio dottrinale, diviene opportuno chiedersi se le condotte di realizzazione e diffusione del *malware WannaCry* evidenzino l'inottemperanza agli obblighi di prevenzione e repressione imposti agli Stati. In primo luogo, si discute se lo Stato della Nord Corea abbia diligentemente vigilato al fine di scongiurare l'attacco verosimilmente sviluppatosi all'interno del proprio *cyberspace*[70]. A tal proposito, si ricorda che uno Stato è obbligato ad agire con diligenza al fine di prevenire

---

[66] Lo studio specifico della disciplina della *due diligence* con riferimento alle vicende cibernetiche è stato oggetto di recenti analisi dottrinali. Si richiamano in questa sede gli articoli di E. JENSEN, *State Obligations in Cyber Operations*, in *Baltic Yearbook of International Law*, 2014; R. KOLB, *Reflections on due diligence duties and cyberspace*, in *German Yearbook of International Law*, 2015, 113-128; A. BENDIECK, *Due Diligence in Cyberspace*, in *Stiftung Wissenschaft und Politik German Institute for International and Security Affairs*, 2016, 11-18; R. BUCHAN, *Cyberspace, Non-State Actors and the Obligation to prevent Transboundary Harm*, in *Journal of Conflict & Security Law*, 2016, 429-453; S. SHACKLEFORD, S. RUSSELL, A. KUEHN, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, in *Chicago Journal of International Law*, 2016, 1-50. Anche il *Tallinn Manual 2.0*, cit., dedica attenzione allo studio in esame. Le *rules* 6 e 7 sono appositamente riguardanti il tema della *due diligence* nel *cyberspace*.

[67] Tale approccio è condiviso dal gruppo di redattori del *Tallinn Manual 2.0*, cit., 31. In particolare, per quanto concerne la questione circa i margini di applicabilità di tale regime rispetto alla fattispecie in esame, essi ribadiscono che: «the experts further observed that the due diligence principle has long been reflected in jurisprudence; it is a general principle that has been particularised in special regimes of international law. Since new technologies are subject to pre-existing international law absent a legal exclusion therefrom, they concluded that the due diligence principle applies in the cyber context».

[68] V. *supra*, nota 63.

[69] In questa sede si intende riportare il chiaro ragionamento espresso da M SCHMITT, *In Defence of Due Diligence in Cyber Space*, cit., 73: «in international law, it is unnecessary to identify a distinct reason to apply a general principle in a particular context. On the contrary, since it is a general principle, the presumption is that the principle applies unless state practice or opinio juris excludes it».

[70] Sul complesso ed incerto tema dell'individuazione dei *cyberspace* nazionali, si leggano E. JENSEN, E. TALBOT, *Cyber Sovereignty: The Way Ahead*, in *Texas International Law Journal*, 2015, 275; N. TSAGOURIAS, R. BUCHAN, *op. cit*., 19; *Tallin Manual 2.0*, cit., 11: «The principle of sovereignty applies in cyberspace».

esclusivamente i danni derivanti da condotte di cui esso ha effettiva *conoscenza*[71]. Dal momento che la conoscenza dello Stato non può essere presunta per il semplice fatto che le attività si sono verificate all'interno dei confini statali[72], ne dovrebbe derivare un obbligo in capo ad esso di vigilare in modo da acquisire conoscenza circa le relazioni all'interno del proprio *cyberspace*[73]. Tuttavia, l'obbligo di instaurare una vigilanza finalizzata a conoscere l'evolversi delle vicende all'interno del *cyberspace* presenterebbe evidenti profili di criticità. Lo Stato, infatti, per adempiervi in maniera efficace, dovrebbe esercitare un controllo pressante delle comunicazioni e dell'architettura della rete internet nazionale, andando a configurare un vero proprio meccanismo di sorveglianza sui soggetti che accedono ad essa. Questa soluzione appare in contrapposizione rispetto alle disposizioni del *corpus* normativo dei diritti umani che prescrivono la tutela del diritto alla *privacy*[74]. Come ribadito dal Consiglio per i diritti umani, la rilevanza normativa delle disposizioni volte a tutelare i diritti dell'uomo deve trovare applicazione anche con riferimento alle relazioni informatico-digitali[75].

Il valore sotteso alla tutela della *privacy* nel diritto internazionale sembra essere in grado di escludere la possibilità di richiedere agli Stati (in questo caso alla Corea del Nord) il dovere di controllare il proprio *cyberspace* mediante una sorveglianza costante e capillare della rete internet, limitando conseguentemente l'applicazione degli obblighi di diligenza ai soli casi in cui venga dimostrata l'effettiva conoscenza dello Stato circa il

[71] Si riporta quanto espressamente disposto dalla Corte internazionale di giustizia nella sentenza *Corfù channel*, par. 22: «Albania's obligation to notify shipping of the existence of mines in her waters depends on her having obtained knowledge of that fact in sufficient time before October 22nd ; and the duty of the Albanian coastal authorities to warn the British ships depends on the time' that elapsed between the moment that these ships were reported and the moment of the first explosion».

[72] *Ibidem*, par. 18: «it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew».

[73] *Ibidem*, par. 29: una condotta diligente implicherebbe anche oneri di vigilanza, i quali deriverebbero proprio dall'impossibilità di presumere la conoscenza dello Stato rispetto alle condotte da prevenire e reprimere per il semplice fatto che esse si sono verificate all'interno del proprio territorio. Ad ulteriore conferma di ciò, si riporta in questa sede la definizione di *due diligence* affermata dagli Stati Uniti nel citato caso *Alabama*, par. 572 s.

[74] Il diritto alla *privacy* è qualificato come un diritto umano da un elevato numero di convenzioni internazionali. Tra queste, si ricordano il Patto internazionale dei diritti civili e politici, 1976, art. 17; la Convenzione europea dei diritti dell'uomo, 1950, art. 8; la Convenzione americana dei diritti dell'uomo, 1978, art. 11. Secondo la dottrina maggioritaria, l'importanza ed il seguito di tali disposizioni pattizie codifica la tutela del diritto alla *privacy* anche come norma consuetudinaria**.**

[75] Consiglio dei diritti umani, risoluzione del 5 luglio 2012, UN Doc. A/HRC/17/27. Il tema del delicato rapporto tra l'utilizzazione delle reti informatiche e la tutela dei diritti umani è approfondito da G.M. RUOTOLO, *Internet (diritto internazionale)*, cit., 561-564.

verificarsi delle vicende cibernetiche anomale[76]. Nel caso in questione, non vi è alcuna certezza che la Corea del Nord fosse a conoscenza della preparazione dell'attacco informatico. Conseguentemente, appare difficile ritenere questo Stato responsabile per la violazione del dovere di diligenza.

Tuttavia, un differente profilo di lesione delle norme di *due diligence* con riferimento all'attacco *WannaCry* potrebbe essere ravvisato. Come precedentemente riportato, il gruppo Lazarus, presunto autore del virus informatico alla base dell'attacco, si sarebbe servito del programma *Eternal Blue*, al fine di diffondere l'attacco *ransomware*[77]. Secondo gli esperti, quest'ultimo era stato precedentemente progettato dall'NSA americana, la quale, tuttavia, ne aveva perso il controllo in seguito ad un attacco informatico nei suoi confronti[78]. Tale specifico aspetto della vicenda appare particolarmente interessante proprio alla luce dell'eventuale sussistenza di obblighi di prevenzione e repressione in capo agli Stati in tema di tutela del *cyberspace*. Ci si interroga in questa sede se gli Stati Uniti d'America, autori di una fondamentale componente del *malware WannaCry*, abbiano ottemperato o meno ad un obbligo di prevenzione rispetto al verificarsi di vicende informatiche dannose.

Sul tema, Brad Smith, presidente dell'ufficio legale di Microsoft, si è esposto, affermando: «An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today nation-state action and organized criminal action»[79]. Di fatto, l'aver creato, a livello governativo, un programma potenzialmente configurabile come "arma informatica", il quale poi è stato sottratto ed utilizzato, appunto, per scopi illeciti, fa sorgere (per lo meno) il dubbio che gli Stati Uniti non abbiano adottato le misure necessarie per evitare la diffusione di tale strumento.

6. L'analisi proposta nel presente lavoro evidenzia le criticità che caratterizzano il tentativo di inquadrare le vicende dell'attacco *WannaCry* nel contesto della disciplina tradizionale in tema di responsabilità degli Stati. Alla luce di ciò, acquisisce particolare rilevanza l'eventuale operatività del principio di *due diligence* nel contesto in esame, al fine di comprendere se sia possibile ravvisare una responsabilità internazionale degli Stati derivante, non tanto dalla commissione dell'attacco, bensì dalla violazione di obblighi preventivi e repressivi rispetto al verificarsi di vicende cibernetiche dannose.

[76] Secondo quanto scritto da N. TSAGOURIAS, R. BUCHAN, *op. cit.*, 69: «knowledge of cyber injurious act could be established only upon the notification by the victim State that has the discretion to select the States from the territories of which injurious transmissions occur».

[77] V. *supra*, par. 2.

[78] V. *supra*, nota 14.

[79] La dichiarazione è del 14 maggio 2017.

A conclusione del presente lavoro, si intende rimarcare alcune considerazioni generali riguardanti il principio di *due diligence* con riferimento al contesto giuridico-fattuale esaminato. In primo luogo, si deve evidenziare che una generale applicazione del principio di *due diligence* non può essere esclusa con riferimento alle vicende cibernetiche. Secondo quanto affermato dalla giurisprudenza internazionale, ogniqualvolta lo Stato esercita la propria sovranità territoriale, esso dovrà comportarsi con diligenza al fine di prevenire e reprimere inaccettabili conseguenze dannose con riferimento ad altri Stati[80]. Dal momento che la gestione del *cyberspace* è oramai considerata dalla pressoché unanimità della Comunità internazionale una manifestazione dell'esercizio della sovranità dello Stato sul territorio[81], l'ottemperanza al principio di *due diligence* deve essere opportunamente garantita dagli Stati anche nel contesto cibernetico.

Tuttavia, la specificazione della diligenza in precisi standard di condotta non sembra ancora essersi sostanziata nella formazione di norme consuetudinarie specificamente applicabili alla materia in esame[82]. L'assenza di un *corpus* normativo atto a concretizzare il generale obbligo di condotta diligente riduce l'effettiva rilevanza del principio in esame, il quale, benché potenzialmente in grado di garantire l'imposizione di obblighi agli Stati finalizzati a ridurre la pericolosità derivanti dal mondo informatico-cibernetico,

[80] Si ricorda, a conferma di tale considerazione, quanto affermato dalla Corte permanente di arbitrato nel lodo del 4 aprile 1928, *Island of Palmpas case* (*USA v. The Netherlands*): «Territorial sovereignty (…) involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war».

[81] Pare opportuno ricordare anche in questa sede che, a conferma di ciò, il *Tallin Manual 2.0*, cit., *rule* 1, 11, afferma: «The principle of sovereignty applies in cyberspace». La tematica dell'estensione della sovranità statale nell'ambito cibernetico è affrontata in maniera estremamente chiara in N. TSAGOURIAS, R. BUCHAN, *op. cit*., 19: «the State can exercise its prescriptive and enforcement jurisdiction over cyberspace and over cyber activities on the basis of nationality and territoriality». Secondo E. JENSEN, E. TALBOT, *Cyber Sovereignty: The Way Ahead*, in *Texas International Law Journal*, 2015, 275: «as a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources».

[82] Dall'analisi delle condotte degli Stati, non sembra riscontrabile un livello di uniformità a livello di prassi tale da poter ritenere che si ravvedano i requisiti richiesti al fine di configurare la formazione di apposite disposizioni consuetudinarie volte a disciplinare precisi parametri di diligenza richiesti ai soggetti internazionali. Solitamente, gli Stati affrontano il tema della *due diligence* nel *cyber context* ciascuno con specifica attenzione alle proprie particolari esigenze. La necessità di controllare e monitorare che il proprio *cyberspace* non sia un terreno fertile per atti illeciti appare un'esigenza a cui gli Stati adempiono mediante approcci differenti. A titolo esemplificativo, si riporta quanto osservato da S. SHACKLEFORD, S. RUSSELL, E. KUEHN, *op. cit*., 34: «The United States is more voluntary, Germany takes a more regulatory approach featuring a comprehensive cybersecurity policy that has long eluded U.S. policymakers, and China's approach encompasses broader economic and national security efforts».

non appare al giorno d'oggi ancora maturo a tal punto da poter adempiere a tale delicato compito.

Tuttavia, è opportuno evidenziare che un ruolo suppletivo in questo campo potrebbe e dovrebbe essere esercitato dal diritto convenzionale. A tal proposito, si osservi che un trattato internazionale sul tema è già stato stipulato. Si tratta della Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[83], che ambisce a fornire una disciplina normativa «necessaria come deterrente per azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi, reti ed informazioni, attraverso la criminalizzazione di questi comportamenti, (…), e attraverso l'adozione di poteri sufficienti per combattere realmente questi reati, facilitando la loro individuazione, investigazione e l'esercizio dell'azione penale a livello sia nazionale che internazionale»[84]. Lo studio degli obblighi del Trattato mostra la formazione di un parametro di condotta pattizio di carattere preventivo e repressivo appositamente predisposto per il settore delle offese informatiche[85].

In attesa di evoluzione normativa del diritto internazionale generale, lo strumento dei trattati internazionali risulta essere potenzialmente in grado di colmare le evidenti lacune presenti in materia di *cyber-due diligence*. La formazione di ulteriori disposizioni convenzionali concernenti specifici obblighi di condotta con riferimento alla gestione del *cyberspace* potrebbe garantire, da un lato, una soluzione immediatamente efficace, benché limitata alle parti contraenti del trattato, e, dall'altro, potrebbe incentivare uno sviluppo progressivo del diritto consuetudinario.

[83] La centrale rilevanza di tale Convenzione al fine della progressiva evoluzione del diritto internazionale nell'ambito cibernetico è affermata, *ex multis*, da R. BUCHAN, *Cyberspace, Non-State Actors*, cit.; T. YAMIN, *Combating Cyber Terrorism Through an Effective System of Cyber Security Cooperation*, in *Terrorism Experts Conference*, 2015, 9; E. JENSEN, *State Obligations in Cyber Operations*, in *Baltic Yearbook of International Law*, 2014, 28-30; G. M. RUOTOLO, *Internet-ional Law*, cit., 66-69.

[84] Cfr. il preambolo di questa Convenzione.

[85] Tuttavia, secondo i più attenti esponenti della dottrina, le fattispecie di reato previste dalla Convenzione in esame non coprono la totalità delle condotte cibernetiche offensive che sono state lanciate in questi anni. Tale lacuna ne limita evidentemente la portata applicativa. In tema, v. l'opinione di R. BUCHAN, *Cyberspace, Non-State Actors*, cit.: «these international legal regimes do not comprehensively address all forms of malicious cyber conduct that violate the international legal rights of other states and consequently there will be many instances where states continue to look to the customary international law obligation upon states to prevent transboundary harm for protection».

ABSTRACT

The WannaCry Case: The Phenomenon of Cyber Attacks in the Context of the International Responsibility of the States

The cyber attack *WannaCry*, which occurred in May 2017, caused serious damages to international private companies and to more than 150 States located all over the world. After a preliminary description of the facts related to the attack, this article aims to frame it under the law of the international responsibility of States. More precisely, the objective and the subjective elements of the international wrongful act must be identified in the case at stake. Conclusively, by observing the extreme difficulty in attributing WannaCry's conducts to a State, the article points out the potential relevance of the application of the general principle of due diligence in cyberspace, in order to find a juridical deterrent to the production and proliferation of malwares on the internet.