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

Attività ostili nel ciberspazio: il quadro normativo internazionale e dell'UE e l'importanza di istituire un'Unità congiunta per il ciberspazio

Annita Larissa Sciacovelli
Professoressa aggregata di Diritto dell'Unione europea, Università degli Studi di Bari Aldo Moro

1. Introduzione: le attività ostili perpetrate nello spazio cibernetico. L'intensità, la sofisticazione e la pervasività degli attacchi informatici[1] compiuti a danno di entità critiche (pubbliche e private) nel panorama internazionale ha spinto l'Unione europea a dotarsi di una politica e di una strategia della cibersicurezza[2].

A fronte delle profonde vulnerabilità tecnologiche di sistemi e reti dell'informazione e della comunicazione, il legislatore europeo ha previsto un quadro di azioni coerenti relative agli aspetti normativi, operativi, diplomatici e di difesa della cibersicurezza. Esso è rivolto a garantire il funzionamento del Mercato unico[3] e la protezione della sovranità digitale[4], anche alla luce dei crescenti investimenti degli Stati nelle *cyber capabilities* offensive, non solo per scopi militari.

La finalità perseguita dall'Unione è strutturare una risposta rapida, efficiente ed efficace alle azioni offensive da attuare sulla base di un coordinamento politico, tecnico e operativo e attraverso strumenti innovativi, tra i quali spicca la proposta di istituzione di un'Unità congiunta sul ciberspazio.

Premessa essenziale all'esame di tale proposta e, in generale, della politica e strategia europea sulla cibersicurezza, è la conoscenza delle caratteristiche dello spazio cibernetico, delle principali attività ostili compiute in Rete e degli obblighi internazionali degli Stati.

---

[1] V. Parlamento europeo, *Recenti attacchi informatici e strategia di sicurezza informatica dell'UE per il decennio digitale*, giugno 2021, www.europarl.europa.eu, e *Rapporto Clusit* 2021, clusit.it. Per attacchi cibernetici si intendono: «[M]alicious cyberoperations entailing the use of deliberate actions and operations to alter, disrupt, deceive, degrade or destroy computer systems or networks, or otherwise undermine the confidentiality, integrity, and availability of computer systems or networks for individuals and communities»; così H.S. LIN, *Offensive Cyber Operations and the Use of Force*, in *Journal of National Security Law and Policy*, 2010, p. 4 ss. Per una visione d'insieme della problematica in Italia v. Camera dei deputati, *Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber*, 2019, p. 8, emi.camera.it.

[2] V. *State of the Union: Commission Proposes a Path to the Digital Decade to Deliver the EU's Digital Transformation by 2030*, digital-strategy.ec.europa.eu.

[3] V. Commissione europea, Alto Rappresentante dell'Unione per gli affari esteri e la politica della sicurezza, *Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, 7 febbraio 2021, Join(2013) 1 final, p. 2.

[4] V. Sulla nozione di sovranità riferita al ciberspazio, G.P. CORN, R. TAYLOR, *Sovereignty in the Age of Cyber*, in *American Society of International Law*, 2017, p. 207; M.N. SCHMITT, L. VIHUL, *Tallin Manual 2.0, The International Law Applicable to Cyber Operations*, Cambridge, 2017, p. 12 ss., Rule 4, secondo cui «[c]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law» sul presupposto che «States enjoy sovereignty over cyber infrastructure, persons, and cyber activities located on their territory. This includes both public and private cyber infrastructure». V. anche J. POHLE, *Digital Sovereignty*, in *Internet Policy Review*, 2020; in termini generali sull'evoluzione della nozione di sovranità nel diritto internazionale, E. CANNIZZARO, *La sovranità oltre lo Stato*, Bologna, 2020, p. 25.

Per ciberspazio si intende quel luogo fisico e virtuale composto dall'insieme delle infrastrutture informatiche interconnesse a livello globale e che si caratterizza per l'assenza di confini fisici[5]. In proposito, si rammenta la duplice natura delle operazioni condotte nello spazio cibernetico, che possono essere volte o a realizzare attività ostili verso sistemi informatici di Stati, enti pubblici o privati e individui, o a svolgere ordinarie funzioni di sorveglianza a protezione dei sistemi medesimi, specie quelli strategici, per garantire la sicurezza dello Stato[6].

Autori di tali operazioni sono *hackers* che agiscono sia indirettamente, mettendo a disposizione della criminalità le piattaforme digitali reperibili sul *Dark web* usando il sistema di navigazione *Tor*, sia direttamente sferrando attacchi *ransomware* o inserendo *malware* (*software* maligni) nei sistemi operativi di enti (pubblici o privati) per criptare, esfiltrare o distruggere i dati e le informazioni in essi contenuti, ovvero per renderli inutilizzabili[7].

Oltre a perseguire finalità estorsive – o anche politicamente o eticamente motivate – gli *hackers* svolgono attività di cyber spionaggio industriale o militare, suscettibili di causare danni rilevanti alla *digital economy* e alla difesa del Paese[8].

Attualmente, lo spazio cibernetico rappresenta il quinto dominio della difesa militare che, a differenza degli altri spazi (terrestre, marino, aereo e spaziale), è stato creato dall'uomo. In tale spazio gli attacchi mirano ad alterare le relazioni economiche e geopolitiche fra Stati[9] e, nello specifico, a minare la loro sicurezza, il loro sviluppo economico e sociale e anche i diritti umani fondamentali[10].

Occorre ricordare che le operazioni cyber possono essere compiute anche per finalità terroristiche o per realizzare le c.d. cyber interferenze. Il fenomeno del cyber terrorismo consiste nello svolgimento, sul piano virtuale, di attività di proselitismo, addestramento, incitamento, radicalizzazione e autofinanziamento funzionali alla realizzazione di atti terroristici nel mondo fisico o in Rete[11]. Nel primo caso, la Rete rappresenta il *mezzo*

---

[5] Cfr. V. A.A. DONIS, *International Law on Cyber Security in the Age of Digital Sovreignty*, in *E-Int relations*, 2020, www.e-ir.info; nonché V.P. RIVELLO, *Diritto e spazio cibernetico*, in *Diritto penale e globalizzazione*, 2018, www.dirittopenaleglobalizzazione.it.; A. KASTELIC, *International Cyber Operations*, 2021, p. 1, unidir.org.

[6] V. Assemblea generale, risoluzione del 31 dicembre 2020, A/RES/75/240, p. 2.

[7] Cfr. S. NANNI, *Come cambiano le norme penali con il* cyber crime*: i reati informatici e cibernetici*, 2013, www.agendadigitale.eu; R. FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo: dalla* CIA-Triad Protection *ai più recenti sviluppi*, in *Diritto di Internet*, 2019, p. 443 ss.

[8] V. J. KIRK, *GhostNet Cyber Espionage Probe Still has Loose Ends*, in *Pc World*, 2009, www.pcworld.com, secondo cui il «'legal vacuum' surrounding cyber espionage can be especially problematic for investigators».

[9] V. rapporto del 14 luglio 2021 del UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security (UNGEE), *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. 76/135, par. 6 ss. Cfr. W.J. LYNN, *Defending e New Domain: The Pentagon's Cyber Strategy*, in *Foreign Affairs*, 2010, p. 97; R. AZZARONE, *Cyber vademecum*, in *Gnosis*, 2014, p. 36 ss.

[10] V. M. MENSI, *Sicurezza cibernetica e tutela dei diritti*, in M. MENSI, P. FALLETTA (a cura di), *Il diritto del web*, Milanofiori Assago, 2015, p. 290.

[11] Cfr. R. PINO, *Il "cyberterrorismo": un'introduzione*, in *Ciberspazio e diritto*, 2013, p. 429 s.; D. COHEN, *L'evoluzione del terrorismo contemporaneo nel cyber-spazio*, in *Gnosis*, 2016, p. 118 ss.; P.M. SABELLA, *Il fenomeno del cyber crime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, in *Informatica e diritto*, 2017, p. 141.

per coordinare tali atti, mentre nel secondo caso la manomissione di dati o sistemi operativi rappresenta l'obiettivo stesso dell'operazione. Il fenomeno in esame non è trascurabile specie in considerazione della creazione del "Cyber Califfato" e della "Cyber Jihad". Quest'ultima, in particolare, è impiegata nella raccolta delle diverse frange di estremismo islamico radicalizzato violento.

Il fenomeno delle cyber interferenze consiste nelle operazioni condotte da profili falsi (*trolls*) per attaccare le *info-strutture* di uno Stato al fine di diffondere notizie non veritiere su piattaforme digitali per manipolare l'opinione pubblica o interferire nei processi elettorali di uno Stato[12]. L'obiettivo è quello di incrementare le tensioni socio-politiche e l'instabilità politica degli Stati ledendo i valori fondamentali dello Stato di diritto e dei processi democratici[13]. Tale pratica rientra nella più ampia e diffusa strategia della "guerra ibrida" condotta da alcuni Paesi, fra cui la Federazione Russa e la Cina[14].

A ben vedere, le operazioni cibernetiche possono avere conseguenze gravi non solo in Rete, bensì anche nel mondo fisico; si pensi agli effetti della manomissione e del blocco dei sistemi operativi di centrali elettriche, nucleari o idriche, dei servizi sanitari nazionali[15] o dei sistemi di controllo del traffico aereo, ciò che potrebbe causare conseguenze paragonabili all'attacco alle torri gemelle del 2001[16].

Gli esempi riportati testimoniano che le operazioni in parola non solo violano la sovranità digitale dello Stato, ma addirittura ne minacciano la sicurezza, come è accaduto nel 2007 in Estonia[17]. Si tratta del primo caso di compromissione delle funzionalità dei servizi essenziali di uno Stato con un attacco DDoS (*Distributed Denial of Service*) che ha paralizzato quasi l'intera infrastruttura informatica. Successivamente, un attacco

[12] V. L. DE ROCHEGONDE, É. TENENBAUM, *Cyber-influence: les nouveaux enjeux de la lutte informationnelle*, in *Focus stratégique*, Ifri, 2021, p. 48 ss., spire.sciencespo.fr.

[13] V. rapporto del 14 luglio 2021, cit., par. 9 ss.

[14] V. G. CHAZAN, *La Germania protesta contro la Russia per l'ondata di attacchi informatici*, in *Financial Times*, 6 settembre 2021, www.ft.com.

[15] Si pensi al *ransomware* condotto dal gruppo criminale informatico russo *Wizard Spider*, il quale ha bloccato i sistemi operativi del Servizio sanitario irlandese, interrompendo l'assistenza sanitaria in tutto il Paese e con gravi conseguenze per la salute e la vita dei cittadini, v. *Irish Hospitals Are Latest to Be Hit by Ransomware Attacks*, giugno 2021, www.nytimes.com. Altri attacchi sono stati messi a segno contro importanti aziende chiedendo il pagamento di migliaia o addirittura milioni di dollari in Bitcoin. Negli Stati Uniti, ad esempio, uno dei principali oleodotti (*Colonial Pipeline*) nel maggio 2021 ha annunciato l'interruzione del funzionamento del sistema operativo per mano di gruppo di *hackers* – noti come *DarkSide*, anch'essi presumibilmente operanti dal territorio russo – portando al blocco dei rifornimenti di gasolio. Per il Presidente statunitense Biden si tratta di un'attività ostile che, insieme ad altri, mina la sicurezza nazionale, v. *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, 2021, www.whitehouse.gov.

[16] V. ampiamente M. COHEN, F. CHUCK, G. SIBONI, *"Four Big "Ds" and a Little "r": A New Model for Cyber Defense*, in *Cyber, Intelligence, and Security*, 2017, p. 21 ss.

[17] L'attacco è stato sferrato in concomitanza con la decisione del Governo estone di rimuovere dalla piazza principale di Tallinn la statua di bronzo del milite ignoto sovietico, da cui la sua imputazione alla Federazione Russa sulla base di altri elementi raccolti dall'*intelligence*; v. R. SHACKELFORD, *An Introduction to the Law of Cyber War and Peace*, in *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge, 2014, p. 263; I. ZAHRA, I. HANDAYANI, D.W. CHRISTIANTI, *Cyber-attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law*, in *Yustisia*, 2021, p. 48.

analogo è stato sferrato contro la Georgia nel 2019[18], in concomitanza con il conflitto con la Federazione Russa.

Quanto fin qui detto spiega il motivo per cui la quasi totalità delle recenti attività ostili (specie tra Stati) si svolge nello spazio cibernetico. Quest'ultimo, infatti, garantisce l'anonimato dei *cyberactors* nonché la rapidità e l'economicità dell'operazione, specie se paragonata al costo sostenuto per l'acquisto di armamenti convenzionali.

Uno dei principali problemi dei cyber attacchi riguarda la punizione dei "cyber actors": si tratta di gruppi criminali o entità non statali, che spesso godono della tolleranza o sponsorizzazione di Stati. Qualora sia possibile provarne il coinvolgimento, anche gli Stati possono essere ritenuti internazionalmente responsabili in base al processo di attribuzione[19].

In realtà, le autorità statali incontrano non poche difficoltà nello svolgimento delle indagini per individuare i responsabili materiali e i mandanti di attacchi cibernetici poiché si tratta di attività illecite transnazionali che sono compiute in (e da) Stati (Iran, Cina, Federazione Russa e Corea del nord, per citare i principali). Tali difficoltà sono di natura tecnico-giuridica e riguardano principalmente il piano probatorio (*digital forensic*)[20]. Infatti, al fine di cancellare le prove necessarie alla loro identificazione (*fingerprint*), gli *hackers* coordinano migliaia di attacchi simultanei tramite *bot-net* che sono collegati a una molteplicità di sistemi informatici, situati in diversi Paesi e appartenenti a terzi, i quali sono ignari del loro coinvolgimento nel disegno criminoso[21].

A ciò si aggiunga la mancanza di una convenzione internazionale sugli obblighi a carico degli Stati per le operazioni ostili condotte (o tollerate o sponsorizzate) nel ciberspazio e l'assenza di strumenti di cooperazione giudiziaria internazionale, se non in ambiti regionali e relativi all'obbligo di repressione dei reati informatici[22]. In Europa, ad esempio, vige la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001[23], aperta agli Stati terzi e che si segnala per l'efficienza nella cooperazione transfrontaliera e perché rappresenta un modello normativo di armonizzazione del diritto e della procedura penale. Di recente è stato adottato il progetto del secondo Protocollo addizionale alla citata Convenzione, relativo alla cooperazione sulla

---

[18] V. P. ROGUSKI, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 2020, www.justsecurity.org.

[19] V. E.M. MUDRINICH, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, in *Air Force Law Review*, 2012, p. 167; K.E. EICHENSEHR, *The Law & Politics of Cyberattack Attribution*, in *UCLA Law Review*, 2020, p. 67.

[20] J.S. DAVIS II, *Stateless Attribution: Toward International Accountability in Cyberspace*, 2017, p. 9 ss., www.rand.org; C. PAYNE, L. FINLAY, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, in *George Washington International Law Review*, 2017, p. 49 ss.

[21] Si pensi all'attacco cyber WannaCry lanciato dalla Corea del Nord e che, nel maggio 2017, rapidamente infettò più di 230.000 computer in più di 150 Paesi, colpendo, fra gli altri, il sistema sanitario nazionale britannico, il Ministero degli interni russo, la compagnia spagnola Telefonica, la francese Renault e la società FedEx. Cfr. White House, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, 2017, www.whitehouse.gov.

[22] V. la risoluzione del 22 gennaio 2001 dell'Assemblea generale che invita gli Stati a «eliminate safe havens for cybercriminals», par. 1(a), U.N. Doc. A/RES/55/63.

[23] Essa è entrata in vigore il 1° luglio 2004 ed è stata ratificata da 66 Stati, tra cui l'Italia; v. Cybercrime Convention Committee, *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, 2020, T-CY (2020)16, www.coe.int.

criminalità informatica e all'accesso alle prove elettroniche nelle indagini penali (anche in *Cloud*) che, una volta entrato in vigore dovrebbe avere un significativo impatto a livello globale[24].

2. Cenni al quadro normativo internazionale di riferimento. La mancanza di una disciplina internazionale in materia di cibersicurezza ha portato la Comunità internazionale ad assumere un duplice approccio riguardo all'individuazione dei principî applicativi del *cyber international law*, inteso quale complesso normativo che regola i rapporti tra gli utenti all'interno del ciberspazio[25]. Infatti, inizialmente vi era una polarizzazione tra due orientamenti: uno favorevole alla redazione di nuovi principî e l'altro all'applicazione in via analogica di principî vigenti nel diritto internazionale. Attualmente, prevale l'ultima impostazione, senza preclusione per l'elaborazione di obblighi addizionali, ove necessario[26].

Tale impostazione trova conferma nel progetto del codice internazionale di condotta per la sicurezza delle informazioni[27] e nei rapporti redatti dai due gruppi di lavoro[28] che, parallelamente, in seno all'ONU si occupano di individuare le norme che formano il *cyber international law* e che hanno adottato una serie di rapporti, di cui l'ultimo nel 2021, «sul comportamento responsabile degli Stati nel cyber spazio nel contesto della sicurezza internazionale»[29].

Si tratta di atti di *soft law* che ricostruiscono il quadro normativo che regolamenta il cyber spazio ricorrendo al diritto internazionale generale, ai principî contenuti nella Carta dell'ONU, al diritto internazionale dei diritti umani e al diritto internazionale umanitario[30]. Nello specifico, nei rapporti sono richiamati i principî del rispetto della sovranità territoriale o dell'indipendenza politica degli Stati[31]; del divieto della minaccia o dell'uso della forza; della non ingerenza negli affari interni di uno Stato; dell'obbligo di soluzione

[24] Il secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica include misure e salvaguardie per migliorare la cooperazione internazionale fra le autorità giudiziarie e fra le autorità e i fornitori di servizi in altri Paesi. La Commissione europea vi ha partecipato, v. Decisione del Consiglio del giugno 2019, rif. 9116/19.

[25] V. A. SARDU, *L'*international cybersecurity law*: lo stato dell'arte*, in *La Comunità Internazionale*, 2020, p. 5.

[26] V. rapporto del 14 luglio 2021, cit., par. 16 ss.

[27] La proposta del Codice è stata redatta da Cina, Russia, Tagikistan e Uzbekistan e sottoposto all'Assemblea generale che è pubblicata nella risoluzione del 13 gennaio 2015, UN Doc.AG/RES/69/723.

[28] L'individuazione del diritto internazionale applicabile alle attività nel ciberspazio è condotta sia dal UN Open-ended Working Group on Development in the Field of Information and Telecommunications in the Context of International Security (OEWG), creato dall'Assemblea generale nel 2018 e costituito da venticinque esperti, sia dal UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security (UNGEE) creato dall'Assemblea generale nel 2004, al quale partecipano gli Stati membri dell'ONU interessati. A ciò si aggiunga l'attività del Open-ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study of the Problem of Cybercrime, istituito nel 2019.

[29] Per il Segretario generale dell'ONU si tratta di attività "complementari"; v. la lettera del 14 luglio 2021 sul rapporto del 2021 del UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security, A/76/135, 4.

[30] Sul valore del *soft law* nella formazione del diritto internazionale si rinvia a G. SCALESE, *La problematica dei c.d. "accordi non vincolanti" nel diritto internazionale: un potenziale paradosso*, in *Rivista della cooperazione giuridica internazionale*, 2017, 9 ss.

[31] V. art. 2 del Codice citato.

pacifica delle controversie e dell'obbligo degli Stati di impedire che sul loro territorio si svolgano attività illecite, per citare i principali[32].

Un obbligo analogo ricade anche sugli Stati di "transito" di tali attività, la qual cosa comporta che lo Stato che esercita la propria giurisdizione sulle attività svolte nel proprio territorio e sulle infrastrutture cibernetiche ha l'obbligo di vigilare secondo la (*cyber*) *due diligence*[33].

In entrambi i casi le autorità statali devono adottare misure efficaci e ragionevoli per porre termine a tali attività[34] e fornire assistenza nella fase investigativa e nella persecuzione degli *hackers*, senza che ciò implichi il monitoraggio di *tutte* le attività informatiche sul territorio[35]. In proposito, un utile strumento per la cooperazione internazionale potrebbe essere la Convenzione delle Nazioni Unite sul contrasto al crimine transnazionale organizzato del 5 novembre 2000[36].

In questo contesto, maggiormente complesso risulta il processo di attribuzione delle operazioni ostili ad uno Stato e l'accertamento della sua responsabilità internazionale, in quanto comporta l'esame di importanti e delicate considerazioni di natura tecnica, giuridica e politica[37]. Non a caso nella risoluzione dell'Assemblea generale dell'ONU dell'11 dicembre 2018 l'indicazione che un'attività illecita sia riconducibile (o originata) dal territorio di uno Stato (o da sue infrastrutture) di per sé è insufficiente ai fini dell'attribuzione[38], salvo che non vi sia una chiara evidenza probatoria[39]. In proposito, occorre segnalare l'assenza nel diritto internazionale di garanzie e standard uniformi e imparziali nella raccolta delle prove digitali e di regolamenti e procedure circa lo svolgimento di un "equo" processo di attribuzione. Per il Gruppo di esperti dell'ONU è opportuno agire con

[32] V. rapporto del 14 luglio 2021, cit., norma 13, lett. f), par. 43, come già affermato, in termini generali, dalla Corte internazionale di giustizia nella sentenza del 9 aprile 1949, *Canale di Corfù*, *Regno Unito* c. *Albania*, par. 22. V. anche Assemblea generale, risoluzione del 5 ottobre 2020, *Advancing Responsible State Behaviour in Ccyberspace in the Context of International Security*, A/C.1/75/L.4, 2 ss. In dottrina, v. E.T. JENSEN, *Cyber Warfare and Precautions Against the Effects of Attacks*, in *Texas Law Review*, 2010, p. 88; M.C. WAXMAN, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal International Law*, 2011, p. 36; O.A. HATHAWAY, *The Law of Cyber-Attack*, in *California Law Review*, 2012, p. 817.

[33] Cfr. S.J. SHACKELFORD, 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, p. 8.

[34] V. rapporto del 14 luglio 2021, cit., principio 30, lett. a), s.

[35] *Ibidem*, norma n. 13, lett. c), par. 30 ss.; principio 71, lett. b) e c).

[36] V. gli articoli 5, 7, 11 e 13 della Convenzione, che è stata ratificata da 190 Stati ed è entrata in vigore il 29 settembre 2003.

[37] V. rapporto del 14 luglio 2021, cit., par. 71, lett. c). Per info o segnalazioni su incidenti o attacchi sponsorizzati da Stati v. Council on foreign relations, *Cyber Operations Tracker*, www.cfr.org/cyber-operations.

[38] *Ibidem*, principio 71, lett. g).

[39] V. risoluzione dell'Assemblea generale dell'ONU dell'11 dicembre 2018, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/73/27, par. 1.2. In dottrina, M.J. SKLEROV, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, in *Military Law Review*, 2009, p. 12, favorevole alla responsabilità oggettiva dello Stato; W. HEINTSCHEL VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace,* in *International Law Studies*, 2013, p. 123; M. ROSCINI, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in *Texas International Law Journal*, 2015, p. 233 ss.; M. FINNEMORE, D.B. HOLLIS, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 2019, papers.ssrn.com.

cautela per evitare che vi siano equivoci e che vi sia il rischio di un'*escalation* di tensione tra Stati[40].

In proposito, dato lo scarso sviluppo del diritto internazionale in materia di attribuzione, potrebbe essere utile il ricorso all'art. 8 del Progetto di articoli della Commissione di diritto internazionale sulla responsabilità internazionale del 2001 per decidere dell'imputabilità allo Stato di attività di agenti *di fatto* o di entità non statali sottoposte alla sua giurisdizione o al suo controllo, sia esso effettivo o indiretto o generale[41].

Peraltro, nel caso in cui l'attacco cibernetico assuma proporzioni ed effetti tali da minacciare la pace e la sicurezza internazionale, è pacifico l'esercizio del diritto naturale alla legittima difesa individuale e collettiva (art. 51 della Carta ONU) e l'operatività del sistema di sicurezza collettiva della Carta dell'ONU (art. 39 ss. Carta ONU). Analogamente, la NATO riconosce che al verificarsi di tale ipotesi sia consentito il ricorso alla capacità difensiva collettiva anche ibrida, cioè inclusiva dell'impiego di armi cibernetiche e cinetiche *ex* art. 5 del suo Statuto[42].

Un altro problema riguarda l'applicazione dello *jus in bello* all'impiego di armi cibernetiche a seguito di attacco cibernetico o "ibrido", cioè condotto usando anche armi cinetiche[43]. Sul punto, vi è grande attenzione per l'elaborazione del *cyber warfare* alla luce della complessità della disciplina. Si pensi alla nozione di "attacco", che nel diritto internazionale umanitario sembra essere limitata alla nozione di atto di violenza[44], o all'applicazione dei principî di precauzione, di proporzionalità, di necessità e di distinzione[45] tra obiettivi militari e civili [46]. È ben noto che solo i primi possono essere bersaglio di un attacco armato, la qual cosa pone il problema della liceità di un cyber attacco, atteso che le reti commerciali sono impiegate anche dal settore militare[47]. Risulta quindi quanto

---

[40] V. rapporto del 14 luglio 2021, cit., par. 22.

[41] V. W. BANKS, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, in *Texas Law Review*, 2017, p. 1487 ss. Sulle nozioni di controllo effettivo, generale e indiretto operato dallo Stato nei confronti di agenti di fatto ed emerso nel diritto e nella giurisprudenza internazionale, v. J. KURBALIJA, *State Responsibility in Digital Space*, in *Swiss Review of International and European Law*, 2016, p. 15; 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 and Security Law*, 2016, p. 14.

[42] V. art. 5 dello Statuto della NATO del 4 aprile 1949, www.nato.int. Cfr. G.M. RUOTOLO, Internet-ional law. *Profili di diritto internazionale pubblico della rete*, Bari, 2012, p. 20 ss.; M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to the Cyber Warfare*, Cambridge, 2017, II ed., p. 24 ss.; E.D. BORGHARD, S.W. LONERGAN, *Cyber Operations as Imperfect Tools of Escalation*, in *Strategic Studies Quarterly*, 2019, p. 122 ss.

[43] Cfr. JT. BILLER, M.N. SCHMITT*, Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare*, in *International Law Studies,* 2019, p. 180.

[44] V. l'art. 49(1) del I Protocollo dell'8 giugno 1977 addizionale alle quattro Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime di conflitti armati internazionali. Cfr., ICRC, *31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31IC/11/5.1.2, pp. 4 e 36 ss.; ICRC, *International Humanitarian Law and Cyber Operations During Armed Conflicts*, position paper, 2019, p. 3 ss.

[45] V. art. 57 del I Protocollo addizionale.

[46] V. art. 52(1)(2) del I Protocollo addizionale. Per una discussione sul tema v. M.N. SCHMITT, *Rewired Warfare: Rethinking the Law of Cyber Attack*, in *International Review of the Red Cross*, 2014, p. 189; ID., *Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations*, in *International Review of the Red Cross*, 2019, p. 102.

[47] V. H.A. HARRISON DINNISS, *The Nature of Objects: Targeting Networks and the Challenge ofDefining Cyber Military Objectives*, in *Israel Law Review*, 2015, p. 39; K. MAČÁK, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law,* ivi, p. 55; M.N. SCHMITT, *The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive Precision*, ivi, p. 81.

mai impellente l'avvio di un processo di negoziazione di una "Convenzione di Ginevra" che disciplini l'applicazione dei citati principî alle attività nel ciberspazio in tempo di pace[48].

Di recente, l'Assemblea generale ha promosso anche la creazione di un Comitato per l'elaborazione di un progetto di Convenzione internazionale relativa al contrasto dell'uso delle tecnologie della informazione e comunicazione per finalità illecite, che inizierà i lavori nel gennaio 2022 e che garantirà l'avvio di procedure decisionali partecipative della società civile e dei principali *stakeholders* internazionali[49]. Sul punto, molte sono le questioni da discutere; si pensi, ad esempio, al problema della legittimità della cyber *pre-emptive self defence* e alla qualificazione di cyber-mercenari delle società che svolgono operazioni di *cyber offence* per conto degli Stati per motivi tecnici e di risparmio economico, sostenuta dal Gruppo di lavoro dell'ONU sui mercenari[50].

3. La strategia e la politica sulla cibersicurezza dell'Unione europea e la proposta di un'Unità congiunta per il ciberspazio. In questo contesto, la partecipazione dell'UE alle attività e alle proposte in seno all'ONU sulla cibersicurezza risponde alla comune esigenza di garantire un ciberspazio globale, stabile e sicuro[51]. Questo, infatti, è ritenuto indispensabile per favorire una trasformazione digitale sicura dell'economia e della società europea[52] e per affrontare le nuove sfide di servizi e prodotti digitali, quali i *Cloud*, il 5G e l'intelligenza artificiale[53].

Nelle conclusioni dell'8 ottobre 2021 su "Esplorare il potenziale dell'iniziativa concernente un'Unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala"[54], il Consiglio UE ha condiviso il quadro giuridico proposto dall'ONU sulla disciplina relativa al *comportamento responsabile* degli Stati nel ciberspazio, richiamando i citati principî di diritto internazionale.

Nello specifico, dal 2001 la politica di sicurezza delle reti e dell'informazione[55] è uno degli obiettivi della Commissione europea perseguiti sia con l'istituzione

[48] Come proposto dal presidente statunitense Joe Biden al *summit* di Ginevra di giugno 2021 con il presidente della Federazione Russa Putin, v. D.A. SANGER, *Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons*, in *NY Times*, 15 luglio 2021, www.nytimes.com. V. Rapporto del 14 luglio 2021, cit., p. 18.

[49] V. la risoluzione dell'Assemblea generale del 24 maggio 2021, *Countering the Use of Information and Communications Technologies for Criminal Purposes*, UN Doc. A/75/L.87/Rev. 1.

[50] V. il rapporto del Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, *The Human Rights Impact of Mercenaries, Mercenary-Related Actors and Private Military and Security Companies Engaging in Cyberactivities*, UN Doc. A/76/151, par. 6. Cfr. T. MAURER, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, 2018, p. 31.

[51] V. Commissione europea, Alto Rappresentante dell'Unione per gli affari esteri e la politica della sicurezza, *Comunicazione congiunta al Parlamento europeo*, cit., p. 2.

[52] V. A. BENDIEK, E. PANDER MAAT, *The EU's Cybersecurity Policy: Building a Resilient Regulatory Framework*, in G. SIBONI, L. EZIONI (eds.), *Cybersecurity and Legal-Regulatory Aspects*, Tel Aviv, 2021, p. 23.

[53] Cfr. Consiglio UE, la Relazione del 16 dicembre 2020 sull'impatto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G, SWD(2020) 357 final.

[54] V. conclusioni del Consiglio dell'8 ottobre 2021, Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala, Doc. 12534/21, par. 8.

[55] Nel 2001 la Commissione ha adottato la comunicazione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" (COM(2001) 298 def.); nel 2006 ha adottato "Una strategia per una società

dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[56], sia con la prima Strategia sulla cibersicurezza nel 2013[57]. Le priorità strategiche ivi individuate, tutt'oggi attuali, riguardano lo sviluppo di capacità industriali e tecnologiche; la creazione di una politica internazionale coerente sul ciberspazio e lo sviluppo di una politica e di una capacità di resilienza e di ciberdifesa connessa alla Politica di sicurezza e di difesa comune.

Successivamente, nel 2016 si è proceduto all'adozione della direttiva sulla sicurezza delle reti e dei sistemi informativi[58] (direttiva NIS) al fine di garantire un elevato livello comune di cibersicurezza in tutta l'UE. La direttiva in parola rappresenta il punto di partenza nella gestione del rischio perché introduce requisiti di sicurezza obbligatori per i principali operatori economici che forniscono servizi essenziali e per i fornitori di alcuni dei principali servizi digitali[59]. Grazie alla citata direttiva, la cooperazione tra gli Stati membri in materia di cibersicurezza è garantita dal Gruppo di cooperazione NIS e dalla Rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT).

Di recente, la crescente diffusione dei dispositivi connessi ai sistemi operativi, c.d. "internet degli oggetti" (IoT), ha spinto il legislatore europeo a proporre la direttiva "NIS2", volta a favorire la resilienza in *tutti* i settori esclusi dalla precedente versione[60]. Contestualmente, stante il mutato ecosistema della cibersicurezza, nel dicembre 2020 la Commissione europea e l'Alto rappresentante per gli affari esteri e la politica della sicurezza hanno presentato una nuova Strategia dell'UE per la cibersicurezza, inclusiva di strumenti normativi, strategici e di investimento per costruire un'Europa resiliente e digitale.

Obiettivi fondamentali della Strategia in parola sono il raggiungimento dell'autonomia strategica, intesa quale capacità di compiere scelte autonome nel settore mantenendo un'economia aperta, il potenziamento della *leadership* digitale e il rafforzamento delle capacità strategiche dell'UE.

Il Consiglio ha ulteriormente precisato i settori d'intervento dell'attuale *decennio digitale* tra i quali – oltre alla revisione della direttiva sulla resilienza dei soggetti critici[61]

---

dell'informazione sicura" (COM(2006) 251). Dal 2009 la Commissione ha sviluppato un piano di azione e una comunicazione "Proteggere le infrastrutture critiche informatizzate" (COM(2009) 149 def.), approvata dalla risoluzione del Consiglio 2009/C 321/01 e COM(2011) 163, e dalle conclusioni del Consiglio 10299/11.

[56] V. il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, cui sono seguiti altri regolamenti di revisione, di cui l'ultimo è il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

[57] V. la comunicazione congiunta della Commissione europea e del Servizio europeo per l'azione esterna, Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN(2013) 1 final.

[58] V. la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[59] V. la comunicazione della Commissione, Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza, COM(2016) 410 final.

[60] V. la proposta del 16 dicembre, COM(2020) 823 final.

[61] V. la proposta di direttiva sulla resilienza dei soggetti critici, COM(2020) 829 final.

e del regolamento relativo alla resilienza operativa digitale[62] – particolare attenzione è dedicata alla creazione dell'Unità congiunta per il ciberspazio. A tal fine, nelle citate conclusioni di ottobre 2021 esso ricostruisce il quadro normativo di riferimento richiamando i principî di sussidiarietà, proporzionalità, complementarità, non duplicazione e riservatezza e la natura esclusiva della competenza statale in materia di sicurezza nazionale (art. 4, par. 2, TUE). È fatta salva la competenza degli organi dell'UE qualora si tratti di incidenti e crisi di cibersicurezza su vasta scala che ledano il corretto funzionamento del Mercato unico e la sicurezza interna dell'UE.

L'Unità in esame è stata ritenuta essenziale dalla Presidente della Commissione europea, Ursula von der Leyen, già nelle Linee guida per la Commissione europea 2019-2024[63], per dotare l'UE e gli Stati membri di una risposta *coordinata* in situazioni di emergenza dovute ad attacchi e incidenti di carattere transfrontaliero.

A tale Unità spetterà pertanto il compito di coinvolgere gli esperti delle comunità della cibersicurezza per costruire una "consapevolezza situazionale condivisa" (riferita alla decisione di attribuzione di un attacco informatico), nonché la gestione e la mitigazione delle crisi informatiche dell'UE. Essa coordinerà anche i meccanismi di assistenza, su richiesta di uno o più Stati membri, integrando i meccanismi orizzontali e settoriali di risposta alle crisi dell'UE già esistenti. Il riferimento è all'allineamento di meccanismi e processi esistenti in ambito statale ed europeo, con particolare riguardo alle procedure di cooperazione e di condivisione delle informazioni esistenti a tutti i livelli necessari – tecnico, operativo, strategico/politico e diplomatico[64] – tra Stati membri[65] e tra istituzioni, organi e agenzie dell'UE[66].

L'operatività dell'Unità è prevista a partire dal 30 giugno 2022 grazie alla creazione di una piattaforma virtuale e fisica[67] e di un Comitato dell'UE per lo sviluppo delle capacità informatiche[68]. A tal proposito, il Gruppo di lavoro orizzontale sulle questioni

[62] V. la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) N. 600/2014 e (UE) n. 909/2014, COM(2020) 595 final; proposta di direttiva che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE 2016/2341, COM(2020) 596 final.

[63] V. Ursula von der Leyen, Linee guida politiche per la prossima Commissione europea 2019-2024, 16 luglio 2019.

[64] V. la comunicazione congiunta al Parlamento europeo e al Consiglio, Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale, del 23.6.2021, JOIN(2021) 14 final.

[65] Si pensi al Gruppo di cooperazione NIS e alla rete di CSIRT, alla rete delle organizzazioni di collegamento per le crisi informatiche fra cui la *Cyber Crisis Liaison Organisation Network* (CyCLONe), alla cooperazione strutturata permanente e volontaria (PESCO) che ha portato alla creazione di "gruppi di risposta rapida agli incidenti informatici"; alla *task force* di azione congiunta contro la criminalità informatica (J-CAT) e alla rete giudiziaria europea per la criminalità informatica (EJCN).

[66] Il riferimento è alla cooperazione tra ENISA e CERT-UE, al memorandum d'intesa tra l'ENISA, l'Agenzia europea per la difesa (AED) e il Centro europeo di competenza per la cibersicurezza, istituito con il regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento, per citare i più significativi.

[67] V. la raccomandazione (UE) 2021/1086 della Commissione, del 23 giugno 2021.

[68] V. EU CyberNet, *The Bridge to Cybersecurity Expertise in the European Union*, 28 ottobre 2021, www.eucybernet.eu.

informatiche dell'UE ha invitato l'Unione e gli Stati membri a impegnarsi nello sviluppo del quadro europeo sugli obiettivi e possibili ruoli e responsabilità dell'Unità[69].

Da un punto di vista operativo, l'Unità e i centri operativi di sicurezza (SOC2) costutuiranno una Rete che entro il 2023 rappresenterà il *ciberscudo* europeo. A tal fine, l'Unità sarà competente a individuare precocemente i segnali di attacchi informatici, grazie all'impiego di strumenti basati sull'intelligenza artificiale, in collaborazione con la rete CSIRTS, l'ENISA e il Cybercrime Centre (EC3) creato presso EUROPOL.

Poiché l'Unità lavorerà a stretto contatto con l'ENISA, è il caso di specificare il diverso ruolo svolto dai due organi. Infatti, mentre gli obiettivi dell'ENISA riguardano l'assistenza alle istituzioni dell'Unione e agli Stati membri nel potenziare e condividere la capacità informatiche per prevenire, rilevare e rispondere a problemi e incidenti di sicurezza delle reti, stimolando una cooperazione tra attori del settore pubblico e privato, l'Unità si occuperà di cooperazione tecnica e operativa in caso di incidenti anche transfrontalieri, sul presupposto di una mappatura delle capacità disponibili a livello nazionale e dell'UE e dopo aver valutato le strategie nazionali sulla cibersicurezza, anche per evitare la duplicazione delle attività [70].

In conclusione, la creazione dell'Unità risponde all'obiettivo primario dell'Unione di dotarsi di una *bussola strategica* per costruire un'Europa indipendente da un punto di vista militare, economico e tecnologico e anche per realizzare le priorità di resilienza, sovranità e autonomia tecnologica. In tal senso, essa rappresenta un passo importante verso la creazione di un esercito dell'UE, sempre che la sua attività si basi su un approccio olistico, poiché la sicurezza informatica è un dominio interdisciplinare[71].

A tal fine, che tra i compiti dell'Unità dovrebbe essere previsto, sotto la direzione dell'AED, il sostegno agli Stati membri nella creazione di una forza militare di cyber difesa proattiva e reattiva[72]; il rafforzamento della capacità di *digital investigation*, sulla quale è già impegnata la Commissione europea[73]; la conduzione di operazioni di contrasto agli attacchi cyber terroristici e alle info-strutture in collaborazione con l'EUROPOL.

Per la realizzazione dei compiti indicati l'Unità dovrebbe potersi avvalere dell'ausilio di un *Hub* di cyber *intelligence* degli Stati membri e dell'Unione (atteso che l'attuale Centro UE di analisi e di intelligence-INTCEN ha funzione meramente consultiva),

[69] V. Consiglio UE, Progetto di conclusioni sull'esplorazione del potenziale dell'iniziativa Joint Cyber Unit - complementare alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su larga scala, par. 23, 6 ottobre 2021.

[70] V. comunicazione congiunta della Commissione e dell'Alto rappresentante per gli affari esteri e la politica di sicurezza sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, del 16 dicembre 2020, JOIN (2020) 18 final.

[71] V. T. AMADOR, *Enhancing Cyber Defense Preparation Through Interdisciplinary Collaboration, Training, and Incident Response*, in *Journal of The Colloquium for Information Systems Security Education*, 2020, p. 5, cisse.info/journal/index.php/cisse/article/download/130/130.

[72] V. Parlamento europeo, *Report on the State of EU Cyber Defense Capabilities*, (2020/2256(INI)), 2021.

[73] Cfr. R.A. Wessel, *European Law and Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *International Law and Cyberspace*, Cheltenham, 2021, p. 123 ss.

affinché siano raccolte e valutate le minacce informatiche in Europa grazie alla sinergia tra difesa e agenzie di informazione.

Dicembre 2021