BlogDUE

Cyberattacks: ipotesi di reazioni

Andrea Bianco (Dottorando di ricerca in diritto dell'Unione europea – Università degli Studi di Napoli Suor Orsola Benincasa) – 24 febbraio 2023

SOMMARIO: 1. Premessa. - 2. La legittima difesa. - 3. L'art. 5 Patto NATO. – 4. L'art. 42 TUE. - 5. L'art. 222 TFUE. - 6. L'Unione europea e la cyber-sicurezza. - 7. *Segue*. - 8. Conclusioni.

1. I *cyberattacks* che hanno segnato i primi giorni di febbraio hanno riacceso i riflettori su uno strumento bellico sempre più diffuso ed idoneo a produrre un impatto particolarmente grave sulla vita degli Stati (ENISA *Threat Landscape*, 2022). Ad enfatizzare i rischi connessi a tali attacchi, l'Estonia ha affermato che gli stessi risultano comparabili al blocco dei porti di due secoli fa (NATO Parliamentary Assembly, *NATO and Cyber Defence*, 173 DSCFC 09 E bis, 2009, para. 25, 59).

Per inquadrare la tematica, occorre ricordare che l'Agenzia per la Cibersicurezza Nazionale ha rilevato il primo attacco, il 5 febbraio 2023, da parte del Csirt-It, verso diversi paesi del mondo, tra cui la Francia che è risultato il paese più colpito (ACN, Comunicato stampa del 5 febbraio 2023, www.acn.gov.it/notizie/contenuti/rilevato-lo-sfruttamento-massivo-della-cve-2021-21974-in-vmware-esxi). Anche nel nostro Paese, sebbene nessun settore critico sia stato danneggiato, è stata sollecitata, dalla Presidenza del Consiglio, l'adozione di misure di protezione per i settori più sensibili.

Un secondo attacco cibernetico è stato registrato il 13 febbraio, contro numerosi siti internet web della NATO. Ancora, il 21 febbraio, diversi siti web italiani sono stati attaccati dal gruppo hacker filorusso NoName057, che ha rivendicato l'attacco sui propri canali Telegram.

Secondo le prime indagini, tali attacchi non sarebbero stati perpetrati da uno (o più) Stato(i) ma, al contrario, da hackers privati, al fine di richiedere un riscatto.

Invero, non si tratta di un fatto raro od originale, giacché la prassi ha già registrato casi in cui i *cyberattacks* siano sferrati da privati.

La reazione a tali attacchi è affidata in prima istanza agli strumenti tipici del diritto penale e del diritto amministrativo, ma giocano un ruolo chiave anche il diritto internazionale e quello dell'Unione europea.

Più in dettaglio, per quanto riguarda il diritto internazionale, sebbene sia auspicabile che la comunità internazionale reagisca in via accentrata, attraverso gli strumenti offerti dalla Carta delle Nazioni Unite, il multilateralismo imperfetto dell'ultimo ventennio impone di continuare a

ragionare in termini di legittima difesa individuale e collettiva (P. FERRARA, *La sicurezza dell'Europa e la difesa europea nel mondo multipolare: sfide, minacce, opportunità*, R. GUALTIERI, J. L. RHI-SAUSI (a cura di), *La difesa comune europea dopo il Trattato di Lisbona*, Bologna, 2011, p. 33 ss.). L'azione dell'Unione europea in materia di *cybersecurity* va analizzata poi alla luce degli artt. 42 TUE e 222 TFUE.

2. Cominciando l'analisi dal livello internazionale, c'è da chiedersi se cyberattacchi legittimino, in assenza dell'intervento del Consiglio di Sicurezza, una reazione in legittima difesa.

Sul punto, la dottrina ha elaborato diverse considerazioni.

In primo luogo, viene fatto osservare che, un cyberattacco, pur non sostanziandosi in una violazione del divieto di uso della forza, corrisponde ad una violazione del diritto internazionale, cui lo Stato leso, potrà rispondere con contromisure pacifiche. È questo il caso, ad esempio, di un attacco cibernetico volto ad influenzare i risultati elettorali di un altro Stato (United Nations General Assembly, *OEWG in the field of information and telecommunications in the context of international security*, 10 marzo 2021), che sicuramente viola la *domestic jurisdiction* di uno Stato leso, senza però tradursi in un attacco armato.

In secondo luogo, è stato affermato che un cyberattacco, se analogo, in termini di *scale and effect*, ad un attacco cinetico, legittima una reazione in legittima difesa, con strumenti cibernetici o tradizionali (C. FOCARELLI, *Diritto Internazionale*, Vicenza, 2021, p. 628 ss.). La possibilità di qualificare una condotta come attacco armato, infatti, lungi dal dipendere dal tipo di arma utilizzata (parere della Corte internazionale di giustizia dell'8 luglio 1996, *Nuclear Weapons*), discende dagli effetti da essa prodotti, secondo il l'interpretazione della CIG nella sentenza *Nicaragua* (A. STIANO, *Il ricorso agli attacchi informatici da parte della Russia e il ruolo del Diritto internazionale*, in *SIDIBlog*, 2022).

In materia di *cyberattacks*, la dottrina ha altresì individuato criteri volti a classificare un attacco "cibernetico" sulla base di requisiti di portata ed effetti. Così, secondo autorevoli autori un attacco cibernetico, per considerarsi "armato", dovrebbe integrare sette caratteri: "1) Severity, 2) Immediacy, 3) Directness, 4) Invasiveness, 5) Measurability, 6) Military Character, 7) Presumptive legitimacy" (M. N. SCHMITT, *Computer Network Attack and the Use of Force in International Law. Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, vol. 37, 1999, p. 18).

Deve precisarsi altresì che, ai sensi del diritto consuetudinario, la reazione in legittima difesa deve rispettare i principi di necessità e proporzionalità e che la sua finalità deve essere strettamente volta a respingere l'attacco, senza assumere connotati punitivi (Y. DINSTEIN, *Computer Network Attacks and Self-Defence*, in *International Law Studies*, vol. 76, 2002, p. 100 ss.). Consentita è pure la legittima difesa collettiva, che vede uno Stato intervenire in sostegno dello stato vittima dell'attacco; necessaria, a tal fine, è la richiesta di intervento formulata dallo Stato leso.

Con riguardo alla legittima difesa, viene in rilievo un ulteriore problema, connesso al soggetto autore dell'attacco. Il diritto consuetudinario, infatti, ammette una legittima difesa contro attacchi perpetrati da Stati, mentre più problematico risulta il caso di attacchi realizzati da attori non statali, come pare essere l'attacco del 3 febbraio scorso. Sul punto, gli Stati hanno elaborato diverse teorie, caratterizzate da un'interpretazione estensiva della Carta ONU, quali quella dello Stato "unwilling o unable" a contrastare la condotta di attori non statali presenti nel suo territorio, ovvero la "pinprick theory" (M. ROSCINI, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, in A. VON BOGDANDY, R. WOLFRUM (eds.), *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, p. 86 ss.). Tali teorie, utilizzate specialmente per giustificare l'utilizzo degli strumenti del diritto internazionale in reazione agli attacchi terroristici, sono state avallate da una prassi sempre più permissiva rispetto alla legittima difesa contro attori non statali.

Analoghe giustificazioni teoriche possono utilizzarsi in materia di cybersecurity. Vale a dire che un attacco cibernetico, se idoneo ad integrare gli standard di portata ed effetti tipici dell'attacco armato, consentirebbe allo Stato leso di reagire *ex* art. 51.

3. Passando invece all'ipotesi di legittima difesa collettiva, si ricorda che l'articolo 5 del Patto Atlantico collettivizza il problema della sicurezza, stabilendo che un attacco armato contro una delle parti sarà considerato come diretto contro tutte. E, nell'ipotesi in cui tale attacco si concretizzasse, la norma impegna le parti a prestare assistenza allo Stato leso, nell'esercizio del diritto di legittima difesa individuale e collettiva, intraprendendo "such action as it deems necessary, including the use of armed force" (art. 5).

La norma considerata configura perciò un obbligo di assistenza, che può – ma non necessariamente deve – tradursi in un sostegno armato, in legittima difesa collettiva.

Con specifico riguardo ai *cyberattacks*, l'articolo 5 potrebbe trovare applicazione se congiuntamente si verificasse un attacco armato, che, però, si considera sussistente solo nell'ipotesi di uso della forza caratterizzata da un particolare livello di intensità, in termini di portata ed affetti (Y. MIADZVETSKAYA, R. A. WESSEL, *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox,* in *europeanpapers.eu*, vol. 7, n. 1, 2021, p. 413 ss.).

In assenza di tale presupposto, potranno venire unicamente in rilievo le diverse forme di cooperazione previste dal Patto (art. 4). Tale interpretazione è avallata dal Summit di Varsavia del 2016 (North Atlantic Council, Warsaw Summit Communiqué, 8-9 luglio 2016), dove il Consiglio del Nord Atlantico ha affermato che gli attacchi cibernetici rientrano a pieno nel "domain of operations in which NATO must defend itself". Nella stessa prospettiva si pone l'analisi del Group of Experts 2012, secondo il quale "[t]he next significant attack on the Alliance may well come down a fibre optic cable" (NATO 2020, Assured Security; Dynamic Engagement, Analysis and

Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17 maggio 2010).

Sul punto, rileva il caso dell'Estonia, Stato parte del Patto dal 2004, che nel 2007 subì un imponente attacco cibernetico, attribuito alla Federazione Russa. In quell'occasione, l'atteggiamento della NATO fu molto ambiguo; infatti, alla luce degli atti citati, le minacce cibernetiche avrebbero dovuto rientrare dell'ambito di operatività dell'articolo 5 del Patto, invece, agli attacchi non seguì una risposta adeguata in attuazione di tale norma. Pare, quindi, ragionevole sostenere che il tipo di reazione dell'Alleanza dipenda dalle scelte del Consiglio dell'Atlantico del Nord, alla luce di "nature, source, scope, and other aspects" dell'attacco (NATO 2020, Assured Security, cit., 2010)

Per quanto riguarda gli attacchi mossi da attori non statali, l'attivazione dell'articolo 5 potrebbe comunque essere giustificata sulla base dell'analogia con il fenomeno del terrorismo. In presenza di un attacco armato, l'obbligo di assistenza potrebbe operare a prescindere dalla qualificazione di diritto internazionale dell'autore della condotta, alla luce del Concetto Strategico del 1999, che riprende, sul punto, l'omonimo documento del 1991.

4. Venendo agli strumenti messi a punto dall'Unione europea avverso i *cyberattacks*, la difesa collettiva è prevista dall'articolo 42 TUE, che, affermando che la politica di sicurezza e difesa comune è parte integrante della PESC, traduce in norma la strategia iniziata con il Vertice franco-britannico di St. Malo, del 1998, volta ad abbandonare le ipotesi di integrazione dell'UEO nell'Unione Europea e diretta a costituire una politica di difesa interamente europea. Tale scelta politica si premura altresì di non pregiudicare gli impegni assunti dagli Stati nella NATO, che resta il fondamento della difesa collettiva degli Stati che ne sono membri, ed affida la direzione della politica di difesa dell'Unione al Consiglio, che delibera all'unanimità, su proposta dell'Alto Rappresentante (S. IZZO, *La politica estera, di sicurezza e di difesa comune*, in G. TESAURO, *Manuale di diritto dell'Unione europea*, a cura di F. FERRARO, P. DE PASQUALE, vol. II, Napoli, 2021, p. 414 ss.).

L'ultimo paragrafo dell'articolo codifica la clausola di difesa reciproca. La norma, in maniera analoga all'articolo 5 del Patto NATO, sancisce un obbligo di assistenza che gli Stati dell'Unione dovranno prestare allo Stato che sia vittima di un'aggressione armata.

Tra le due norme, però, corre una fondamentale differenza: mentre l'articolo 5 del Patto NATO impone un generico obbligo di sostegno, che può tradursi nel supporto armato, l'articolo 42.7 prevede un obbligo di assistere lo Stato leso "by all the means in their power, in accordance with Article 51 of the United Nations Charter". Gli Stati membri dell'Unione sono pertanto obbligati a fornirsi reciproco sostegno armato, nell'ipotesi in cui siano vittima di un attacco armato (L. PALADINI, *La cooperazione strutturata permanente dell'Unione europea: disciplina, prassi e ruolo nell'integrazione in materia di difesa comune,* in *DPCE online*, vol. 40, n. 3, 2019, p. 1905 ss.).

La clausola sancisce così un obbligo particolarmente stringente, che risulta subordinato alla sussistenza di un attacco armato. Come nel caso della Carta delle Nazioni Unite e del Patto NATO, infatti, l'attacco armato risulta quale imprescindibile presupposto per l'applicazione della clausola di legittima difesa collettiva. Ne deriva che la norma potrà applicarsi solo in presenza di una violazione del divieto di uso della forza caratterizzata da portata ed effetti particolarmente intensi (P.B.M.J. PIJPERS, J.F.R. BODDENS HOSANG, P.A.L. DUCHEINE, *Collective Cyber Defence – the EU and NATO Perspective on Cyber Attacks*, in *Amsterdam Law School Research Paper No. 2021-37, Amsterdam Center for International Law No. 2021-13*, 2021, p. 7).

Alla luce di tali considerazioni, in materia di attacchi cibernetici, rilevano, ai fini dell'articolo 42.7, soltanto quelli equiparabili agli attacchi cinetici. Gli attacchi del 3 e del 21 febbraio, al pari di quello sferrato ai server NATO da Killnet, non rientrerebbe quindi nel novero delle fattispecie coperte dalla norma.

Con riguardo alla clausola di mutua difesa, viene in rilievo un ulteriore problema, rappresentato dagli attacchi cibernetici lanciati da attori non statali. Difatti, la norma, non precisa quali soggetti di diritto internazionale possano sferrare una *armed aggression* e, dunque, contro quali aggressori sia ammesso – ed anzi doveroso, ai sensi del TUE – reagire in legittima difesa collettiva. Sul punto, alla luce del carattere particolarmente stringente dell'obbligo di mutua difesa, ed altresì alla luce degli obiettivi e dei valori sanciti dagli articoli 2, 3 e 22 TUE, pare ragionevole adottare un'interpretazione estensiva e ritenere che la nozione di attacco armato prescinda dalla natura dell'autore dello stesso (J.F.R. BODDENS HOSANG, P.A.L. DUCHEINE, *Implementing Article 42.7 of the Treaty On European Union: legal foundations for mutual defence in the face of modern threats*, in *Amsterdam Law School Research Paper No. 2020-71, Amsterdam Center for International Law No. 2020-35*, 2020, p. 6).

D'altronde, l'estensione dell'ambito di applicazione della legittima difesa, nel diritto internazionale, agli attacchi posti in essere da attori non statali pare confermare tale conclusione.

Come affermato, però, la norma deve considerarsi comprensiva dei soli *cyberattacks* che integrino un vero e proprio attacco armato, data anche la sua non invocazione in conseguenza degli attacchi subiti dalle istituzioni nazionali ed europee sino ad oggi.

5. Nell'ipotesi di attacchi cibernetici che non siano attacchi armati, potrebbe allora assumere rilevanza la clausola di solidarietà, sancita dall'articolo 222 TFUE, secondo il quale gli Stati membri agiscono congiuntamente "in a spirit of solidarity", nell'ipotesi in cui uno di essi subisca un attacco terroristico ovvero sia vittima di una calamità naturale o causata dall'uomo. In tali ipotesi, l'Unione si obbliga a impiegare tutti i mezzi a sua disposizione, compresi quelli militari, per supportare lo Stato vittima dell'evento o dell'attacco. Gli Stati membri, coordinandosi nel Consiglio, prestano altresì assistenza a tale Stato.

Invero, la norma potrebbe essere adeguata a configurare un'ipotesi di supporto in presenza di un attacco cibernetico che non raggiunga la soglia di intensità necessaria ad integrare un attacco armato, ma produca conseguenza di particolare intensità (J.F.R. BODDENS HOSANG, P.A.L. DUCHEINE, *op. cit.*).

Al fine di favorire la corretta applicazione della norma, il Consiglio ha adottato la Decisione 2014/415 del 24 giugno 2014, che per espressa previsione (Art. 2) non ha implicazioni in materia di difesa, ma concerne ipotesi di disastro naturale o causato dall'uomo e di terrorismo.

Prendendo in considerazione, per quanto qui di interesse, l'ipotesi di calamità causata dall'uomo, ai sensi della decisione 2014/415, per disastro si intende una situazione suscettibile di produrre un forte impatto su "people, the environment or property, including cultural heritage". In tale nozione potrebbe rientrare, attraverso un'interpretazione estensiva, la fattispecie di *cyberattacks*, che non corrispondano ad attacchi armati o terroristici (J.F.R. BODDENS HOSANG, P.A.L. DUCHEINE, *op. cit.*, p. 12).

Peraltro, considerando che l'assistenza va prestata ad uno Stato membro "sul suo territorio", pare ragionevole ritenere che tale espressione sia comprensiva dello "spazio digitale", pienamente rientrante nella *domestic jurisdicion* degli Stati (A. M. MARTINO, *the "Solidarity Clause" of the European Union –Dead Letter or Enabling Act?,* in *SIAK-Journal − Journal for Police Science and Practice*, vol. 6, 2016, p. 44).

La maggiore elasticità dello strumento di cui all'articolo 222 TFUE rispetto alla clausola di mutua difesa lo rende più facilmente adattabile e, perciò, invocabile in ipotesi di *cyberattacks*; anche perché, sotto il profilo delle conseguenze della sua attivazione, comporta un generico obbligo di sostegno ed assistenza tra gli Stati membri dell'Unione.

6. In materia di cybersicurezza, l'Unione è comunque intervenuta su diversi fronti, soprattutto per rafforzare la cooperazione tra gli Stati (F. GATTA, *L'Unione europea sotto (cyber)attacco: strategie e prospettive in tema di ciberresilienza e cibersicurezza*, in *rivista.eurojus.it*, 2022).

In questa prospettiva, di recente, Commissione europea, ha rilevato il carattere limitato dell'attuale cooperazione operativa tra gli Stati membri ed ha auspicato l'estensione della stessa, *anche nel contesto dell'articolo 42, paragrafo 7* [TUE] *e dell'articolo 222* [TFUE], enfatizzando il ruolo del settore privato e facendo riferimento al concetto di "cibersolidarietà" (COM JOIN(2022)49 final, 10 novembre 2022).

A ben vedere, la comunicazione si pone in linea con la Strategia per la cyber sicurezza del 2020 (COM JOIN(2020)18 final, 16 dicembre 2020) che, tra i principali obiettivi, annovera lo sviluppo della resilienza e della tutela della "technological sovereignty", il miglioramento delle capacità di prevenzione, deterrenza e reazione e la cooperazione con gli attori statali e privati, coerentemente con la Bussola per il digitale (COM(2021)118 final, 9 marzo 2021), che enfatizza il ruolo trasversale delle tecnologie digitali rispetto alle politiche europee.

Nello stesso contesto si pone altresì la comunicazione relativa al Report sulla EU Security Union Strategy (COM(2022)745 final, 13 dicembre 2022), con la quale la Commissione, preso atto della diffusione e della pericolosità degli attacchi cibernetici, prende in considerazione il fenomeno sia con riguardo alla violazione del principio di non ingerenza, in merito *al* settore della difesa sia rispetto alle fattispecie del terrorismo e del cybercrime. Più precisamente, l'esecutivo UE ha inteso così favorire il dialogo tra le istituzioni europee, gli Stati e gli attori privati, al fine di promuovere lo sviluppo delle capacità cibernetiche e digitali dell'Unione.

De jure condendo, assume poi importanza la proposta di regolamento della Commissione (COM(2022)454 final, 15 settembre 2022), volta ad introdurre requisiti comuni di cybersicurezza, per ridurre la vulnerabilità nei prodotti digitali, ed a favorire la trasparenza e dell'informazione verso i consumatori. La proposta detta taluni "cybersecurity requirements", intesi a migliorare le capacità di difesa dei prodotti digitali da attacchi cibernetici.

Anche il Parlamento europeo ha fatto riferimento al concetto di sicurezza cibernetica, nella risoluzione sulla sicurezza nell'area del partenariato orientale (risoluzione del Parlamento europeo sulla sicurezza nell'area del partenariato orientale e il ruolo della politica di sicurezza e di difesa comune, P9 TA(2022)0236, 8 giugno 2022). La stessa istituzione ha poi adottato una risoluzione sulle ingerenze straniere in tutti i processi democratici nell'Unione europea (risoluzione del Parlamento europeo sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione, P9 TA(2022)0064, 9 marzo 2022), relativa agli attacchi cibernetici idonei a perpetrare una violazione della *domestic jurisdiction* degli Stati dell'Unione, interferendo illegittimamente nei processi elettorali nazionali. Il documento si pone in linea con il Report del National Intelligence Council americano (NIC, *Foreign Threats to the 2020 US Federal Elections*, 10 marzo 2021), che afferma la sussistenza di tentativi russi di interferenza, perpetrata con strumenti cibernetici, nelle elezioni del 2020.

Molto significativo è altresì il ruolo dell'ENISA, che, dal 2004, contribuisce a favorire lo sviluppo di un elevato livello comune di cybersicurezza in Europa. L'azione trasversale della stessa l'ha resa un elemento imprescindibile della strategia europea in materia di cybersecurity (L. LONARDO, *EU Law Against Hybrid Threats: A First Assessment*, in *europeanpapers.eu*, vol. 6, n. 2, 2021, p. 1075 ss.).

Sul punto, assume rilievo il regolamento (UE) 2019/881, che rafforza il mandato dell'ENISA ed istituisce un European cybersecurity certification framework, al fine di rafforzare la capacità dell'Unione di far fronte a *cyber threats*.

7. Sul piano della cooperazione internazionale, con decisione (UE) 2022/895, del 24 maggio 2022, il Consiglio ha autorizzato l'avvio di negoziati, per una convenzione internazionale globale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali.

Infine, in ambito PESC, assume rilievo la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, attraverso la quale il Consiglio dispone misure restrittive che gli Stati possono adottare in risposta ad attacchi cibernetici idonei a produrre effetti significativi, fissando, all'articolo 3, criteri volti a comprendere se un attacco debba ritenersi tale. La decisione, adottata sulla base dell'articolo 29 TUE, rientra nel contesto delle *smart sanctions*, strumento spesso utilizzato dall'Unione per contrastare condotte lesive dei suoi valori ed obiettivi e prevede l'adozione di specifiche misure restrittive mirate, quali il *travel ban* (art. 4) e l'*asset freeze* (art. 5).

A tale atto è conseguita l'adozione, *ex* art. 215 TFUE, del regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri.

8. Al di là dell'importanza delle singole misure sommariamente esaminate, va segnalato che nessuna di esse pare essere uno strumento autosufficiente adeguato a rispondere ai diversi tipi di cyber-attacco, la cui nozione è particolarmente ampia ed incerta (L. LONARDO, *op. cit.*, p. 1093).

Infatti, le diverse forme di attacco cibernetico sono di difficile qualificazione, soprattutto se poste in essere da privati. La loro eterogeneità impone, pertanto, di ragionare *casu casu*, sulle reazioni più adatte al singolo attacco, tanto sotto il profilo dell'efficacia quanto sotto quello della legittimità.

In estrema sintesi, la materia continua a collocarsi tra le sabbie mobili di una disciplina ancora in evoluzione che impone una difficile attività ermeneutica, prestandosi ad interpretazioni abusive e strumentali; ma soprattutto le maggiori difficoltà si rinvengono nell'attività di *attributing*, ossia nella possibilità di affermare con certezza la responsabilità di uno Stato nella commissione di un attacco cibernetico, per ragioni tecniche e politiche (N. KATAGIRI, *Why international law and norms do little in preventing non-state cyber attacks*, in *Journal of Cybersecurity*, vol. 7, n. 1, 2021, p. 3 ss.). Per tali motivi essa continuerà ad essere oggetto di molta attenzione e non soltanto degli addetti.