Diplomazia informatica europea. Prime sanzioni contro i cyber-attacchi e prospettive future

10/08/2020

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, PROSPETTIVE

Roberto A. Jacchia
Marco Stillo

Con una decisione destinata a rimanere nella storia, in data 30 luglio 2020 il Consiglio ha sanzionato[1] sei persone fisiche[2] e tre entità[3] per il loro coinvolgimento negli attacchi informatici che di recente hanno scosso l'opinione pubblica quali, tra gli altri, quello ai danni dell'Organizzazione per la proibizione delle armi chimiche (*Organisation for the Prohibition of Chemical Weapons*, OPCW)[4] nonché quelli noti

[1] Decisione (Pesc) 2020/1127 del Consiglio, del 30 luglio 2020, che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GUUE L 146/2 del 30.07.2020.
[2] Nello specifico si tratta dei sig.ri Gao Qiang, Zhang Shilong, Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Morenets E Oleg Mikhaylovich Sotnikov.
[3] Nello specifico si tratta di *Tianjin Huaying Haitai Science and Technology Development Co. Ltd* (Huaying Haitai), *Chosun Expo* e Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU).
[4] L'OPCW è un'organizzazione internazionale con sede all'Aia che collabora con le Nazioni Unite allo scopo di promuovere e verificare l'adesione alla Convenzione sulle armi chimiche tramite ispezioni di verifica nei paesi membri per assicurare l'adempimento del trattato.

come "*WannaCry*"[5], "*NotPetya*"[6] e "*Oper ation Cloud Hopper*"[7].

Sebbene il ciberspazio offra notevoli opportunità, esso presenta anche nuove sfide per le politiche estere e di sicurezza comune (PESC) dell'Unione. Più particolarmente, negli ultimi tempi si sono registrate sempre più di frequente segnalazioni relative ad azioni di attori pubblici e privati consistenti in attività informatiche dolose che costituiscono atti illeciti ai sensi del diritto europeo. Per sua parte, l'Unione ha progressivamente potenziato la sua resilienza e capacità di prevenzione e risposta nei confronti di tali minacce per salvaguardare la sicurezza e gli interessi europei.

In primo luogo, già in data 19 giugno 2017 il Consiglio aveva adottato un pacchetto di strumenti detti della diplomazia informatica[8], consistente in una disciplina-quadro della risposta comune europea alle attività informatiche dolose con la finalità di incoraggiare la cooperazione, facilitare la riduzione delle minacce a breve termine ed influenzare il comportamento dei potenziali aggressori sul medio-lungo periodo attraverso misure che tenessero conto delle situazioni concrete e fossero proporzionate alla portata, durata e complessità dell'attività illecita in questione.

In data 16 aprile 2018, il Consiglio aveva adottato delle conclusioni sulle attività informatiche dolose ribadendo l'importanza di un ciberspazio globale libero in cui applicare pienamente i diritti umani e le libertà fondamentali, nonché l'impegno europeo per lo sviluppo di norme, regole e principi volontari e non vincolanti per un comportamento responsabile da parte degli Stati Membri. Questi propositi erano stati ulteriormente rafforzati dalle successive conclusioni del 18 ottobre 2018[9].

Infine, in data 17 maggio 2019 il Consiglio aveva adottato il Regolamento 2019/796[10] che, sulla base della Decisione (Pesc) 2019/797[11], istituisce un quadro delle misure necessarie per rispondere agli attacchi informatici con effetti significativi[12], o potenzialmente tali, che costituiscono una minaccia esterna

[5] L'attacco *ransomware* "*WannaCry*" consisteva in un'epidemia di *malware* globale, propagatasi nel mese di maggio 2017 attraverso i computer con sistema operativo *Microsoft Windows*. Più particolarmente, il *malware* ha tenuto in ostaggio i *file* degli utenti, chiedendo poi un riscatto in *Bitcoin* per il recupero dei *file* violati.

[6] "*NotPetya*" è il *malware* nel giugno 2017 ha colpito centinaia di migliaia di computer in Europa, America e Asia e che aveva come bersaglio le reti e i sistemi di medie e grandi aziende quali, tra le altre, *TNT*, *Reckit-Benkiser* e *Maersk*.

[7] L'"*Operation Cloud Hopper*" consisteva una serie di attacchi contro i servizi informatici di multinazionali europee hackerando e utilizzando i dati sensibili a fini commerciali.

[8] Per ulteriori informazioni si veda il seguente LINK.

[9] Per ulteriori informazioni si veda il seguente LINK.

[10] Regolamento (Ue) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GUUE L 129 I/1 del 17.05.2019.

[11] Decisione (Pesc) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GUUE L 129 I/13 del 17.05.2019.

[12] L'articolo 2 del Regolamento 2019/796 dispone: "*... I fattori che determinano se un attacco informatico ha effetti significativi di cui all'articolo 1, paragrafo 1, comprendono:*
a) portata, entità, impatto o gravità delle turbative causate, anche per quanto riguarda le attività economiche e sociali, i servizi essenziali, le funzioni statali essenziali, l'ordine pubblico o la sicurezza pubblica;
b) numero di persone fisiche o giuridiche, entità o organismi interessati;
c) numero di Stati membri interessati;
d) importo della perdita economica causata per esempio mediante furti su larga scala di fondi, risorse economiche o proprietà intellettuale;
e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi;
f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati; o
g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso...".

per l'Unione o i suoi Stati Membri[13]. Le sanzioni previste sono di due tipi. In primo luogo, il congelamento di tutti i fondi e le risorse economiche appartenenti alle persone fisiche o giuridiche coinvolte ed il divieto di metterne altri a loro disposizione o destinarli a loro vantaggio[14], fatte salve le ipotesi di cui agli articoli 4[15] e 5[16]. In secondo luogo, il divieto di ingresso o di

[13] L'articolo 1 del Regolamento 2019/796 ai paragrafi 2-3 dispone: "*... Gli attacchi informatici che costituiscono una minaccia esterna includono quelli che:*
a) provengono o sono sferrati dall'esterno dell'Unione;
b) impiegano infrastrutture esterne all'Unione;
c) sono compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti o operanti al di fuori dell'Unione; o
d) sono commessi con il sostegno, sotto la direzione o sotto il controllo di una persona fisica o giuridica, un'entità o un organismo operanti al di fuori dell'Unione.
A tal fine, gli attacchi informatici sono azioni che comportano:
a) accesso a sistemi di informazione;
b) interferenza in sistemi di informazione;
c) interferenza in dati; o
d) intercettazione di dati,
se tali azioni non sono debitamente autorizzate dal proprietario o da un altro titolare di diritti sul sistema o sui dati o su parte di essi ovvero non sono consentite a norma del diritto dell'Unione o dello Stato membro interessato...".

[14] L'articolo 3 del Regolamento 2019/796 ai paragrafi 1-2 dispone: "*... Sono congelati tutti i fondi e le risorse economiche appartenenti a, posseduti, detenuti o controllati da una qualsiasi delle persone fisiche o giuridiche, delle entità o degli organismi elencati nell'allegato I.*
Non sono messi a disposizione delle persone fisiche o giuridiche, delle entità o degli organismi elencati nell'al legato I, direttamente o indirettamente, fondi o risorse economiche, né sono destinati a loro vantaggio...".

[15] L'articolo 4 del Regolamento 2019/796 dispone: "*... In deroga all'articolo 3, paragrafo 1, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati o la messa a disposizione di taluni fondi o risorse economiche, alle condizioni che ritengono appropriate, dopo aver accertato che i fondi o le risorse economiche in questione sono:*
a) necessari per soddisfare le esigenze di base delle persone fisiche elencate nell'allegato I e dei familiari a loro carico, compresi i pagamenti relativi a generi alimentari, locazioni o ipoteche, medicinali e cure mediche, imposte, premi assicurativi e utenze di servizi pubblici;
b) destinati esclusivamente al pagamento di onorari ragionevoli o al rimborso delle spese sostenute per la prestazione di servizi legali;
c) destinati esclusivamente al pagamento di diritti o spese connessi alla normale gestione o alla custodia dei fondi o delle risorse economiche congelati;
d) necessari per coprire spese straordinarie, a condizione che la pertinente autorità competente abbia notificato alle autorità competenti degli altri Stati membri e alla Commissione, almeno due settimane prima dell'autorizzazione, i motivi per i quali ritiene che debba essere concessa una determinata autorizzazione; o
e) pagabili su o da un conto di una missione diplomatica o consolare o di un'organizzazione internazionale che gode di immunità in conformità del diritto internazionale, nella misura in cui tali pagamenti servono per scopi ufficiali della missione diplomatica o consolare o dell'organizzazione internazionale.
Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del paragrafo 1 entro due settimane dall'autorizzazione...".

[16] L'articolo 5 del Regolamento 2019/796 dispone: "*... In deroga all'articolo 3, paragrafo 1, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati a condizione che:*
a) i fondi o le risorse economiche siano oggetto di una decisione arbitrale emessa anteriormente alla data dell'inserimento della persona fisica o giuridica, dell'entità o dell'organismo di cui all'articolo 4 nell'elenco figurante nell'al legato I, o siano oggetto di una decisione giudiziaria o amministrativa emessa nell'Unione, o di una decisione giudiziaria esecutiva nello Stato membro interessato, prima o dopo tale data;
b) i fondi o le risorse economiche siano usati esclusivamente per soddisfare i crediti garantiti da tale decisione o siano riconosciuti validi dalla stessa, entro i limiti fissati dalle leggi e dai regolamenti applicabili che disciplinano i diritti dei creditori;

transito nel territorio degli Stati Membri, fatte salve le situazioni in cui questi ultimi siano vincolati da un obbligo di diritto internazionale nonché nei casi in cui il viaggio sia giustificato da ragioni umanitarie urgenti, dall'esigenza di partecipare a riunioni intergovernative o a riunioni promosse o ospitate dall'Unione o nell'ambito dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), o sia necessario per l'espletamento di un procedimento giudiziario[17].

La decisione del Consiglio di applicare entrambe le misure restrittive ai soggetti sanzionati conferma dunque gli sforzi europei nella direzione di un ciberspazio globale, aperto e sicuro fondato su una maggiore cooperazione internazionale, in modo da ridurre i rischi di conflitto che possono derivare da incidenti nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC). Ciò che, a sua volta, si traduce nella necessità di un maggiore coinvolgimento degli Stati Membri nell'esercitare la dovuta diligenza e nel prendere le misure appropriate nei confronti dei responsabili di attività informatiche dolose.

c) la decisione non vada a favore di una persona fisica o giuridica, di un'entità o di un organismo elencati nell'allegato I; e
d) il riconoscimento della decisione non sia contrario all'ordine pubblico dello Stato membro interessato.
Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del paragrafo 1 entro due settimane dall'autorizzazione...".

[17] L'articolo 4 della Decisione (Pesc) 2019/797 dispone: "*... Gli Stati membri adottano le misure necessarie per impedire l'ingresso o il transito nello loro territorio di:*
a) persone fisiche responsabili di attacchi informatici o tentati attacchi informatici;
b) persone fisiche che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, oppure agevolandoli per azione o omissione;
c) persone fisiche associate a persone di cui alle lettere a) e b);
elencate nell'allegato.
Il paragrafo 1 non obbliga gli Stati membri a vietare ai loro cittadini l'ingresso nel proprio territorio.
Il paragrafo 1 lascia impregiudicate le situazioni in cui uno Stato membro sia vincolato da un obbligo derivante dal diritto internazionale, segnatamente:
a) in qualità di paese che ospita un'organizzazione intergovernativa internazionale;
b) in qualità di paese che ospita una conferenza internazionale convocata dalle Nazioni Unite o sotto gli auspici di questa organizzazione;
c) in virtù di un accordo multilaterale che conferisce privilegi e immunità; o
d) in virtù del trattato di conciliazione del 1929 (Patti Lateranensi) concluso tra la Santa Sede (Stato della Città del Vaticano) e l'Italia.
Il paragrafo 3 è considerato di applicazione anche qualora uno Stato membro ospiti l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE).
Il Consiglio è debitamente informato in ciascuna delle situazioni in cui uno Stato membro concede una deroga a norma del paragrafo 3 o 4.
Gli Stati membri possono concedere deroghe alle misure stabilite a norma del paragrafo 1 allorquando il viaggio è giustificato da ragioni umanitarie urgenti o dall'esigenza di partecipare a riunioni intergovernative o a riunioni promosse o ospitate dall'Unione o ospitate da uno Stato membro che esercita la presidenza di turno dell'OSCE, in cui si conduce un dialogo politico che promuove direttamente gli obiettivi politici delle misure restrittive, compresa la sicurezza e la stabilità nel ciberspazio.
Gli Stati membri possono anche concedere deroghe alle misure stabilite a norma del paragrafo 1 quando l'ingresso o il transito è necessario per l'espletamento di un procedimento giudiziario.
Uno Stato membro che intenda concedere le deroghe di cui al paragrafo 6 o 7 presenta al riguardo una notifica scritta al Consiglio. La deroga si considera concessa a meno che, entro due giorni lavorativi dalla ricezione della notifica della deroga proposta, vi sia un'obiezione scritta di uno o più membri del Consiglio. Se uno o più membri del Consiglio sollevano obiezioni, il Consiglio, deliberando a maggioranza qualificata, può decidere di concedere la deroga proposta.
Qualora uno Stato membro autorizzi, a norma dei paragrafi 3, 4, 6, 7 o 8, l'ingresso o il transito nel suo territorio delle persone elencate nell'allegato, l'autorizzazione è strettamente limitata ai fini per i quali è concessa e alle persone direttamente interessate...".

Roberto A. Jacchia
PARTNER

r.jacchia@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Marco Stillo
ASSOCIATE

m.stillo@dejalex.com
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com