DICHIARAZIONE DEL G7

SUL COMPORTAMENTO RESPONSABILE DEGLI STATI NEL CYBERSPAZIO

LUCCA, 11 APRILE 2017

INTRODUZIONE

Resta fermo il nostro impegno a favore di un cyberspazio accessibile, aperto, interoperabile, affidabile e sicuro. Riconosciamo gli enormi benefici per la crescita economica e la prosperità che vengono a noi e ad altri dal cyberspazio, quale straordinario strumento di sviluppo economico, sociale e politico.

Siamo preoccupati del rischio di *escalation* e rappresaglie nel cyberspazio, compresi i massicci attacchi di diniego di servizi, i danni a infrastrutture critiche o altre cyber attività con intento doloso che compromettono l'utilizzo e il funzionamento di infrastrutture critiche di erogazione di pubblici servizi. Tali attività potrebbero avere un effetto destabilizzante sulla pace e sulla sicurezza internazionali. Rimarchiamo che il rischio di conflitti tra Stati, conseguenti ad attacchi informatici (TIC), solleva una questione pressante che merita un'attenta considerazione. Esprimiamo, inoltre, crescente preoccupazione per l'interferenza *cyber-enabled* nei processi politici democratici.

Incoraggiamo tutti gli Stati a impegnarsi in comportamenti rispettosi delle leggi e delle norme e che concorrano al rafforzamento della fiducia nel rispettivo uso delle TIC. Approcci collaborativi contribuirebbero anche a lottare contro l'uso del cyberspazio ad opera di attori non-Stato, a scopo terroristico e criminale.

Per queste ragioni, il G7 ha impostato un ambizioso percorso volto alla promozione della sicurezza e della stabilità nel cyberspazio e alla protezione dei diritti umani, attraverso *"I Principi e le Azioni sul Cyberspazio"* approvati a Ise-Shima il 26 e il 27 maggio 2016.

Esortiamo tutti gli Stati a lasciarsi guidare, nel rispettivo uso delle Tecnologie dell'Informazione e della Comunicazione (TIC), dalle raccomandazioni contenute nelle relazioni stilate dai Gruppi di Esperti Governativi delle Nazioni Unite nel Campo dell'Informazione e delle Telecomunicazioni nel Quadro della Sicurezza Internazionale (UN-GGE).

Rinnovando l'impegno a contribuire all'azione di cooperazione internazionale e protezione dai pericoli legati all'uso doloso delle TIC, sosteniamo la seguente Dichiarazione e incoraggiamo altri Stati ad assumere analoghi impegni:

DICHIARAZIONE

Riconosciamo l'urgente necessità di una maggiore cooperazione internazionale, ai fini della promozione della sicurezza e della stabilità nel cyberspazio e dell'adozione di misure intese a ridurre l'uso doloso delle TIC da parte di attori Stato e non-Stato;

Siamo impegnati a promuovere un quadro strategico per la prevenzione dei conflitti, la cooperazione e la stabilità nel cyberspazio, tramite il riconoscimento dell'applicabilità del diritto internazionale esistente al comportamento degli Stati nel cyberspazio, la promozione di norme di comportamento volontarie e non vincolanti in tempo di pace e lo sviluppo e l'attuazione di pratiche Misure di Rafforzamento della Fiducia Informatica (CBMs) tra gli Stati;

Riaffermiamo e approviamo il diffuso assenso, da parte di altri Stati, all'applicabilità del diritto internazionale e, in particolare, della Carta delle Nazioni Unite, all'uso delle TIC da parte degli Stati, affermazione essenziale per il mantenimento della pace e della sicurezza e per la promozione di un ambiente informatico aperto, sicuro, stabile, accessibile e pacifico;

Riaffermiamo altresì che gli stessi diritti di cui gli individui godono quando non sono in Rete, debbano essere tutelati in Rete e ribadiamo l'applicabilità nel cyberspazio del diritto internazionale in materia di diritti umani, compresa la Carta delle Nazioni Unite, il diritto consuetudinario internazionale ed i pertinenti trattati;

Ribadiamo la responsabilità degli Stati di astenersi, nelle relazioni internazionali, dal ricorso alla minaccia o all'uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato o in qualunque altra maniera incompatibile con gli scopi delle Nazioni Unite;

Rileviamo che, ai fini della prevenzione dei conflitti e della pacifica risoluzione delle controversie, il diritto internazionale fornisce anche un quadro per le risposte degli Stati a illeciti che non assumono le proporzioni di un attacco armato – e che possono comprendere cyber attività con intento doloso. Tra le altre risposte legittime, uno Stato che sia vittima di un atto illecito a livello internazionale, può, in talune circostanze, adottare contromisure proporzionate, anche di natura informatica, nei confronti dello Stato che si è reso responsabile dell'illecito, per indurlo ad assolvere agli obblighi internazionali;

Rileviamo che il diritto consuetudinario internazionale in materia di responsabilità di Stato indica gli standard per l' attribuzione di atti agli Stati, che possono applicarsi alle attività nel cyberspazio. A tale riguardo, gli Stati non possono sottrarsi alla responsabilità legale per cyber illeciti perpetrati a livello

internazionale tramite *proxy*. In sede di attribuzione di un illecito internazionale a un altro Stato o di adozione di azioni di risposta, lo Stato dovrà agire in conformità al diritto internazionale. In questo quadro, lo Stato valuterà i fatti e sarà libero di maturare una decisione in linea con il diritto internazionale, con riferimento all'attribuzione di un cyber illecito a un altro Stato;

Nel 2016, abbiamo affermato che, in alcune circostanze, le cyber attività potevano essere assimilate all'uso della forza o a un attacco armato, secondo la Carta delle Nazioni Unite e il diritto consuetudinario internazionale. Abbiamo altresì riconosciuto che gli Stati possono esercitare il diritto naturale di autodifesa individuale o collettiva, sancito dall' Articolo 51 della Carta delle Nazioni Unite, e in accordo con il diritto internazionale, il diritto umanitario internazionale, in risposta a un attacco armato attraverso il cyberspazio;

Per accrescere la predicibilità e la stabilità del cyberspazio, esortiamo gli Stati a chiarire pubblicamente le rispettive posizioni in merito all'applicabilità del diritto internazionale esistente alle attività del cyberspazio, al fine di migliorare la trasparenza e disegnare un quadro di attese di comportamento da parte degli Stati;

Crediamo che le misure di rafforzamento della fiducia sull'uso delle TIC da parte degli Stati siano parimenti essenziali per il consolidamento della pace e della sicurezza internazionali. Sosteniamo lo sviluppo e l'attuazione di tali pratiche Misure di Rafforzamento della Fiducia, compresi i canali di comunicazione tra gli Stati per la gestione delle crisi, in forum bilaterali, regionali e multilateriali, inclusa l'Organizzazione per la Cooperazione e la Sicurezza in Europa (OCSE) e il Forum Regionale dell'ASEAN (ARF);

Sosteniamo altresì la promozione di norme di comportamento volontarie e non vincolanti degli Stati nel cyberspazio in tempo di pace, passibili di ridurre i rischi per la pace, la sicurezza e la stabilità internazionali. Dette norme non vanno intese come limitative o proibitive di eventuali azioni altrimenti in linea con il diritto internazionale, né tanto meno come limitative degli obblighi di uno Stato nel quadro del diritto internazionale, compresi i diritti umani. Riflettono piuttosto le attuali attese della comunità internazionale, fissano gli standard di comportamento di uno Stato responsabile e consentono alla comunità internazionale di valutare le attività e le intenzioni degli Stati, concorrendo a prevenire conflitti in ambito informatico e a promuoverne l'uso pacifico, in vista di una piena realizzazione delle TIC a favore dello sviluppo sociale ed economico globale.

Le seguenti norme di comportamento volontarie e non vincolanti degli Stati in tempo di pace sono contenute nel rapporto GGE del 2015 e nel Comunicato dei Leader del G20 del 2015:

1. In coerenza con gli scopi delle Nazioni Unite, incluso il mantenimento della pace e della sicurezza internazionali, gli Stati dovrebbero cooperare allo sviluppo e all'applicazione di misure che accrescano stabilità e sicurezza nell'uso delle TIC e prevengano pratiche di riconosciuta dannosità o

suscettibili di costituire una minaccia per la pace e la sicurezza internazionali;

2. In caso di attacchi informatici, gli Stati dovrebbero esaminare tutte le informazioni di pertinenza, compreso il più vasto quadro nel quale l'evento si colloca, le sfide di attribuzione in ambiente informatico e la natura e la portata delle conseguenze;

3. Gli Stati non dovrebbero scientemente consentire all'uso del proprio territorio per atti illeciti a livello internazionale, per il tramite delle TIC;

4. Gli Stati dovrebbero vagliare le migliori modalità di cooperazione per scambiarsi informazioni, assistersi reciprocamente, perseguire l'uso terroristico e criminale delle TIC e attuare altre misure di cooperazione per fronteggiare tali minacce. Gli Stati potrebbero dover considerare la necessità di introdurre nuove misure in tal senso;

5. Gli Stati, a garanzia dell'uso sicuro delle TIC, dovrebbero rispettare le Risoluzioni 20/8 e 26/13 del Consiglio per i Diritti Umani in materia di promozione, protezione e godimento dei diritti umani in Rete, nonché le Risoluzioni 68/167 e 69/166 dell'Assemblea Generale sul diritto alla *privacy* nell'era digitale, al fine di garantire il pieno rispetto dei diritti umani, compreso il diritto alla libertà di espressione;

6. Uno Stato non dovrebbe condurre o sostenere scientemente attività informatiche contrarie agli obblighi previsti dal diritto internazionale, che intenzionalmente ledano un'infrastruttura critica o ne compromettano l'uso e il funzionamento ai fini dell'erogazione di pubblici servizi;

7. Gli Stati dovrebbero adottare idonee misure per proteggere la propria infrastruttura critica da minacce informatiche, tenendo conto della Risoluzione 58/199 dell'Assemblea Generale sulla creazione di una cultura generale di cybersicurezza e la protezione di infrastrutture informative critiche, e ogni altra risoluzione di pertinenza;

8. Gli Stati dovrebbero rispondere ad appropriate richieste di assistenza da parte di un altro Stato, la cui infrastruttura critica sia oggetto di attacchi informatici. Dovrebbero altresì rispondere ad appropriate richieste di mitigazione di attività informatiche con intento doloso, indirizzate contro l'infrastruttura critica di un altro Stato che emani dal proprio territorio, nel rispetto della sovranità;

9. Gli Stati dovrebbero adottare misure ragionevoli per assicurare l'integrità della catena di fornitura, in modo tale che gli utenti finali possano riporre fiducia nella sicurezza dei prodotti informatici. Dovrebbero altresì cercare di prevenire la proliferazione di strumenti e techiche informatiche dannosi e l'uso di funzioni dannose nascoste;

10. Gli Stati dovrebbero incoraggiare la responsabile segnalazione di vulnerabilità informatiche e condividere informazioni circa i

corrispondenti rimedi a disposizione, al fine di limitare e possibilmente eliminare minacce potenziali alle TIC e alle infrastrutture che dalle stesse dipendono;

11. Gli Stati non dovrebbero condurre o sostenere scientemente attività lesive dei sistemi informatici delle squadre di risposta alle emergenze autorizzate (o squadre di risposta alle emergenze informatiche o agli attacchi alla cybersicurezza) di un altro Stato. Uno Stato non dovrebbe servirsi delle squadre di risposta alle emergenze autorizzate per condurre illeciti a livello internazionale.
12. Nessun Paese dovrebbe condurre o sostenere il furto di proprietà intellettuale, abilitato dalle TIC, compresi segreti commerciali o altre informazioni commerciali riservate, con l'intento di fornire vantaggi competitivi ad aziende o settori commerciali.