**COMMISSIONE IV**
**DIFESA**

# RESOCONTO STENOGRAFICO

## INDAGINE CONOSCITIVA

**5.**

# SEDUTA DI GIOVEDÌ 28 APRILE 2016

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

## INDICE



**N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo italiani all'Estero: Misto-ALA-MAIE; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI (Unione Sudamericana Emigrati Italiani): Misto-USEI; Misto-FARE ! - Pri: Misto-FARE ! - Pri.**

PRESIDENZA DEL PRESIDENTE FRANCESCO SAVERIO GAROFANI

**La seduta comincia alle 14.45.**

**Sulla pubblicità dei lavori.**

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

**Audizione del professor Andrea Margelletti, presidente del Centro Studi Internazionali (CeSI).**

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del professor Andrea Margelletti, presidente del Centro Studi Internazionali, Ce.S.I.

Saluto il professor Margelletti, che abbiamo già avuto ospite di questa Commissione in numerose altre occasioni e lo ringrazio per aver accolto il nostro invito. Segnalo che il professore è accompagnato dal dottor Francesco Tosato, responsabile del *desk* affari militari del Ce.S.I.

Ricordo che dopo l'intervento del professore darò la parola ai colleghi che volessero porre domande o sollevare interrogativi. Successivamente, il professor Margelletti potrà rispondere.

Senza ulteriori esitazioni passo la parola al professor Margelletti.

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Ringrazio il signor presidente e gli onorevoli deputati presenti. Cercherò amichevolmente di tratteggiare alcune vicende.

L'idea del mio intervento nasce dal cercare di dare un riferimento su quello che sta avvenendo all'estero in materia di *cyber*. Vi sono più scuole di pensiero: *cyber-defence*, *cyber-security* e *cyber-offence*. Inizieremo chiamandola genericamente *cyber*.

Due punti appaiono sempre più evidenti. Il primo è dato da strutture estremamente centralizzate sotto un controllo efficace ed effettivo, perché naturalmente il mondo *cyber*, il mondo virtuale, si muove in un contesto tra il visibile e l'invisibile e questo lascia il rischio di un utilizzo di strutture in maniera meno istituzionale. Dall'altra parte, c'è un volume di risorse dedicate al contesto al momento inimmaginabili per lo standard nazionale.

Cito solo tre esempi in particolare. Non citerò l'esempio statunitense, perché la *magnitudo* è talmente diversa che sarebbe poco garbato. La Francia e la Germania investono nel contesto *cyber* circa un miliardo di euro ciascuna; la Gran Bretagna 3 miliardi di sterline; noi viaggiamo nell'ordine di poco sopra i 150 milioni di euro. Questo vi lascia immaginare quale sia la nostra situazione.

Inoltre, chiunque frequenti il mondo della rete sa perfettamente quanto ormai sia per noi un problema o non essere in campo, nella rete, o addirittura con una velocità bassa. Siamo sempre più affamati e assetati di rapidità. Che cosa hanno fatto le altre Nazioni ?

Hanno creato strutture la cui capacità di risposta è estremamente flessibile. Questa, preparata dai miei collaboratori, è una lastrina che schematizza la capacità di risposta nazionale: come potete immaginare, funziona molto bene in un mondo ideale, dove tutti si parlano, si scrivono e dove c'è

una risposta, ma funziona assai meno bene nel mondo reale, dove c'è bisogno di una velocità impressionante.

Sarò brevissimo, perché la cosa più importante secondo me è, eventualmente, il dialogo con voi. Vi citerò alcuni esempi velocissimi, tra cui quello di Israele, che ha una capacità *cyber* assolutamente avanzata. Tutti voi conoscete e avete sentito parlare di quella che si ritiene verosimilmente una creazione israeliana, cioè Stuxnet, il virus che ha ritardato di alcuni anni il programma nucleare iraniano mandando fuori sincronia di decimi, di millesimi di secondo, le centrifughe per l'accelerazione.

Al suo interno, Israele ha un reparto che è la più grande unità militare israeliana, intendo anche numericamente. Ci sono numerose migliaia di soldati all'interno del servizio di *intelligence* militare israeliano, l'AMAN, che appunto non è una parte dello Stato maggiore, ma proprio un servizio a parte. Anche numericamente è molto più grosso del famoso Mossad. Questo reparto ha una capacità e un *budget* avanzatissimi. Non è un caso che quasi tutte le realtà anche occidentali si servano e acquistino tecnologia israeliana.

La Francia ha avocato nella realtà del servizio esterno – cioè la DGSE, la Direzione generale per la sicurezza esterna, quello che per noi è l'AISE (Agenzia informazioni e sicurezza esterna) – buona parte della componente *cyber*, oltre a un'agenzia interna, un'agenzia nazionale per la sicurezza dei sistemi informativi.

La Germania – parlo sempre della realtà *cyber* – ha portato all'interno del BND, cioè il servizio esterno tedesco, l'AISE francese, più una componente militare molto spinta.

Se, però, vogliamo parlare di sistemi ideali, e io vorrei parlarne e sperare che l'Italia possa averne uno che possa rispondere con efficacia e rapidità alle minacce, probabilmente quelli che hanno l'architettura migliore, ma anche quelli che hanno una storia diversa, sono i britannici. Tutti conoscete l'Agenzia per la sicurezza nazionale, l'NSA americana (*National Security Agency*).

Pensate soltanto che i « supercomputer » a disposizione dell'NSA, che non vendono all'estero come sapete, si calcolano non in centinaia, non in migliaia, ma, presidente, in ettari. La gran parte della *National Security Agency* a Fort Meade si estende sottoterra per chilometri, con una capacità di calcolo immensa, tanto che sono in grado di rompere quasi tutti i codici, perché sono in grado di avere mega-acceleratori che spaccano i codici, per cui riescono a entrare nelle varie comunicazioni.

Questo è qualcosa che gli europei si sognano. Possiamo e dobbiamo fare un lavoro più artigianale, l'importante è, secondo me – abbiamo visto la disparità dei numeri, 150 milioni contro un miliardo di euro – di non buttare al mare le risorse, quelle poche che abbiamo e che avrete la compiacenza di dare al Paese.

La Gran Bretagna ha un servizio esclusivamente dedicato a questo, avendo compreso che il contesto *cyber* ha almeno – consideriamo, se mi passate il termine, la *cyber* come un fiume – tre affluenti principali. Il primo è quello della *cyber-defence*, la protezione dei dati sensibili, delle industrie, delle infrastrutture critiche e, naturalmente, la raccolta. Attraverso il tipo di attacco che si subisce, infatti, si può anche comprendere chi lo sta portando e rispondere adeguatamente.

La seconda parte è quella legata al *cyber-crime*, che conoscete molto meglio di me: le attività di investigazione e monitoraggio della rete da parte delle Forze di polizia, in particolare la Polizia di Stato e l'Arma dei carabinieri.

In ultimo, benché in Italia se ne parli molto poco, il punto fondamentale è la *cyber-offence*. Vogliamo spegnere i radar di un avversario ? Vogliamo minacciare un avversario dicendogli che gli mandiamo in tilt una diga ? Tutta l'attività cinetica di offesa – da noi non se ne parla, si parla solo di *cyber-defence* – ne è una parte. È vero che esiste il porgere l'altra guancia, ma ricordo a tutti voi che di guance ne abbiamo due, e quindi finita la seconda si deve in qualche maniera rispondere.

Gli inglesi hanno una parte fondamentale della *cyber-defence* all'interno del GCHQ (*Government Communications Headquarters*), il quartier generale per le comunicazioni generali, in interazione con il Ministero della difesa. Per essere chiari, lo vedete quotidianamente nelle immagini di al Qaeda, dell'Isis, delle attività clandestine: il campo di battaglia « virtuale » non è più virtuale.

Mentre prima le attività di *cyber* erano, per quanto molto importanti, ancillari a un contesto di confronto fisico, attualmente hanno un peso assolutamente identico; e il *trend* è quello di aumentare questo peso. Che cosa vuol dire ?

Vuol dire che si può vincere una guerra in futuro senza dover uccidere nessuno, ma impedendo tramite attacchi informatici il decollo di aerei. Questo vuol dire che si può inquinare una rete terroristica potendo introdurre all'interno del loro circuito informatico informazioni che portano a far credere che il tuo capo invece è un agente pagato dei servizi di qualche Paese, quindi distruggendoli dall'interno. Questo vuol dire che è possibile monitorare i flussi finanziari illegali, ma è possibile anche, facendo attività di *cyber-offence*, trasformare i flussi finanziari legali in flussi finanziari illegali, di fatto creando un imbarazzo, una criticità o a un individuo o a un'organizzazione o a un Paese. Per fare questo, occorrono risorse economiche, come abbiamo detto più volte, ma soprattutto occorrono strutture snelle.

È per questo che vi propongo qualcosa di profondamente diverso da questo, cercando di razionalizzare la poca moneta che abbiamo e facendo sì che ci sia quel necessario controllo parlamentare su realtà così critiche. Ritengo che sia necessario per l'attività quotidiana delle Forze dell'ordine e delle due agenzie di informazione e di sicurezza, che possono continuare ad avere quelle realtà per le attività di Forze dell'ordine e di quotidianità dell'*intelligence* a supporto delle operazioni dei servizi e che vada compiuto un passo epocale.

Non possiamo continuare a immaginare che ci sia un coordinamento di 150 ministeri che si parlano tra loro quando è già finito tutto con questo schiocco di dita. Ho la fortissima sensazione che dovremo immaginare qualcosa di diverso. Quello che immagino è un servizio, un'agenzia. Io sono uomo dell'antico, quindi li chiamo ancora servizi.

Penso a un'agenzia di *intelligence* con responsabilità *cyber* che abbia due caratteristiche importanti: anzitutto, che sia un'agenzia esclusivamente nazionale, che non dialoghi con servizi omologhi stranieri. Le capacità italiane devono rimanere esclusivamente capacità italiane, e quindi non bisogna mettere a sistema, altrimenti faremmo capire quanto la nostra capacità è avanzata o meno.

In secondo luogo, è necessario, come dicevamo, un controllo, e quindi incastonare quest'agenzia per la *cyber-intelligence* e la *cyber-defence* all'interno dell'architettura dei servizi di informazione e di sicurezza, quindi al pari di AISI (Agenzia informazioni e sicurezza interna), AISE (Agenzia informazioni e sicurezza esterna), e coordinata, come attualmente è per le altre due agenzie, dal DIS (Dipartimento delle informazioni per la sicurezza). Questo permetterebbe un controllo parlamentare a cura del Comitato parlamentare per la sicurezza della Repubblica (Copasir). Dall'altra parte, come per i servizi, ci sarebbe una responsabilità politica netta, chiara e definita, ossia quella del signor Presidente del Consiglio dei ministri.

Abbiamo già, di fatto, un tavolo permanente tecnico. In Italia non abbiamo un Consiglio di sicurezza nazionale, ma qualcosa che vi è abbastanza vicino, ossia il CISR tecnico (Comitato interministeriale per la sicurezza della Repubblica), la parte quotidiana del CISR, che potrebbe essere perfettamente in grado di gestire, in caso di crisi, questa vicenda rapportandosi col Presidente del Consiglio; quindi quanto di più veloce esista, con controllo parlamentare e con realtà definite e incastrate.

Manca la parte della *cyber-offence*, altrimenti non siamo in grado di restituire lo « sganassone » che magari ci hanno dato o non siamo in grado di fare attività a favore del Paese, delle nostre Forze armate, che siano però attività cinetiche. In questo

caso, è molto auspicabile, con tempi che non siano italiani, la realizzazione del comando cibernetico interforze da parte della Difesa. È importante, infatti, nel totale rispetto che ho delle istituzioni, che ci sia sempre, soprattutto in un ambito virtuale, la contezza di chi fa cosa.

Le operazioni offensive, secondo me, dovrebbero continuare a essere fatte, passando dal mondo reale a quello virtuale, coloro che hanno le stellette, le Forze armate, coloro che hanno un ruolo deputato alla difesa della Patria e dell'interesse nazionale. Questa è la mia idea. Naturalmente, bisognerebbe interagire attraverso il Ministro della difesa e il CISR tecnico.

Questo è realizzabile in brevissimo tempo. Certamente, va da parte vostra chiarito il fatto che probabilmente avremo meno passaggi tra un ministero e l'altro, ma dobbiamo renderci conto che il tipo di offesa che ci troviamo davanti ci costringe a modulare le nostre capacità a seconda del confronto che ci si presenta.

Ogni giorno – ciascuno di voi è rappresentativo di un collegio in qualche senso – ci sono giovani che perdono lavoro per questa ragione senza che lo sappiano, perché ci sono società straniere o Nazioni straniere che entrano all'interno delle nostre ditte, fanno *shopping*, e rubano non solo informazioni, ma addirittura i brevetti e li pongono sul mercato qualche minuto prima di noi due che abbiamo fatto società insieme, onorevole. Questo ci rende non solo meno competitivi, che è un problema nazionale, ma credo che sia un problema anche umano di avere tanti giovani che potrebbero avere lavoro e che non ce l'hanno perché non hanno accesso al mondo del lavoro e non sanno perché.

Abbiamo bisogno di una realtà unica, che definisca quali siano i protocolli, che metta il bollino, se mi passate il termine, sull'*hardware* e il *software*. Non è possibile che le aziende private, in alcuni casi pubbliche, vadano così, senza rendersi conto che un problema nazionale prevede una soluzione nazionale e non soluzioni ministeriali o private. Ci vuole un'*authority*, che non può che essere al massimo livello, quindi sotto la Presidenza del Consiglio dei ministri, che abbia il controllo parlamentare, ma anche il ruolo come agenzia di *intelligence* di protezione cibernetica e le capacità per farlo. È un problema di autorevolezza. Al momento, viviamo nel normale, solito, confuso scenario nazionale.

Onorevole, un attimo fa ha preso in mano il telefonino, ce l'ha in questo momento. Lei e io siamo tra i pochi sopravvissuti a un'epoca in cui non c'era il telefono ed esistevano ancora i gettoni. Forse non se li ricorda, ma io ho i capelli bianchi e me li ricordo. Pensi soltanto a che cosa vuol dire come forma di pressione politica all'interno di un voto parlamentare se io estraessi dei dati dal suo telefono, che non è protetto, come non lo è nessuno, o se, oltre a estrarne, ne iniettassi degli altri dicendole: « Questa è la fotografia del tuo telefono, se non mi dai un supporto per questo o per quest'altro, posso crearti una criticità ». Non possiamo più permettercelo. Mentre discutiamo liberamente, forse a volte troppo liberamente, al telefono e abbiamo un atteggiamento troppo disinvolto con i mezzi che utilizziamo per comunicare, dall'altra parte del mondo organizzano strutture. La Cina ha reggimenti per operazioni *cyber*, militari, con tanto di bandiera. Oltretutto, riteniamo che il contesto Cencelli abbia ancora una sua validità.

Credo che sia il momento che tutti noi, voi e io, riconosciamo che dobbiamo piegarci al mondo che avanza, che non è necessariamente quello che ci piace, ma è quello che abbiamo di fronte. Diversamente, il rischio è che riteniamo di essere forti nel mondo reale e siamo spazzati via nel mondo virtuale, che è quello che sempre più troverà spazio. Credo che l'Italia abbia bisogno di razionalità, di spendere bene e di un paio, non di più, di realtà forti, che possano essere veramente efficaci e nelle quali si possa anche, quando si chiede qualcosa, avere la certezza a chi si sta chiedendo per avere delle risposte. Vi ringrazio.

PRESIDENTE. Grazie professor Margelletti per la sua relazione.

Do ora la parola agli onorevoli colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

ANGELO TOFALO. Ringrazio il professore Margelletti, che conoscevo di nome e che per la prima volta ho avuto il piacere di ascoltare.

Sono veramente felice, perché la sua idea è anche la mia. Il momento è quello in cui le risorse economiche sono sempre poche. Lei ha parlato di un miliardo di euro per Francia e Germania, 3 miliardi di sterline per la Gran Bretagna. Più volte ho affermato pubblicamente che, se si vuole fare sicurezza cibernetica in Italia, bisognerebbe investire almeno 1,5-2 miliardi di euro ragionando sul sistema Paese. Gli interessi strategici sono tanti, per cui se si vuol fare qualcosa di serio, di integrazione pubblico-privato, con università, ricerca e piccole medie imprese, 150 milioni di euro non servono a nulla, se non a sistemare – almeno spero – qualche ministero.

Giudico, quindi, il suo modello molto efficace, soprattutto in questa fase di *start-up*, come la chiamo, in cui si inizia a parlare finalmente di sapersi chiudere anche in Parlamento. Spero che, a furia di parlarne, chi oggi è al Governo oggi e chi lo sarà in futuro si diano da fare seriamente.

Sono dell'idea che possa funzionare un'agenzia nazionale sotto il DIS, insieme ad AISI e AISE, quindi specifica per la sicurezza cibernetica. Mi piace anche che abbia pensato a un comando cibernetico interforze della Difesa. Sono al cento per cento d'accordo. So che siamo anche in una fase in cui il Governo sta ragionando per un futuro. Senza voler parlar male di chi è venuto prima, va ricordato come il cosiddetto « decreto Monti » sia stato giusto una traccia, ma forse ha portato più problemi che giovamenti. Spero che chi sta nelle stanze e sta scrivendo qualcosa, tenga presente anche quest'idea. Non aggiungo altro.

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Innanzitutto, ringrazio ancora il presidente per aver deciso di avviare un'indagine conoscitiva su un mondo così complesso e che stiamo ancora esplorando. Non abbiamo ancora idea di quali siano i limiti. Siamo abituati a pensare un mondo con dei limiti fisici. Qui, in realtà, parliamo di un mondo con dei limiti inesplorati. Faccio veramente i complimenti, presidente, per avere avuto il coraggio e la capacità di essere visionario, nell'accezione migliore del termine, per un'indagine in questo contesto.

Mi pongo un problema fondamentale, avendo il privilegio oggi di venire a parlare con voi, che è quello dell'individuazione delle responsabilità in assenza di un confine fisico. Ritengo che la realtà migliore possibile sia quella in cui io so chi sta facendo cosa ed anche chi ha la competenza per cosa. Voi avete la necessità, il dovere, il diritto di chiedere chi sta facendo.

Vedo schemi con venticinque livelli diversi, che probabilmente vanno bene per il mondo della Guerra fredda, cristallizzato, con una tempistica – passatemi l'espressione – da gettone, ma che difficilmente sono realizzabili in un mondo in cui si discute in millesimi di secondo, in cui l'informazione arriva in un attimo e c'è bisogno che venga trasformata e resa per il potere decisionale, per voi, fruibile e comprensibile.

A mio avviso, un centralino con cinquanta bottoni, ognuno di un colore diverso, con una persona che ha la responsabilità di schiacciarne uno, pensando anche che perde il lavoro se schiaccia quello verde anziché giallo o rosso, non è funzionale in un sistema moderno. Ho bisogno che, qualora ci fosse un attacco, ci sia un pulsante solo, schiacciato il quale arrivi un numero di telefono.

Ricordo sempre Henry Kissinger – faccio un passaggio geopolitico se il presidente me lo perdona – quando diceva che non aveva il numero di telefono dell'Europa. Adesso, invece che uno, ne abbiamo decine, ma il problema è lo stesso, e cioè che abbiamo bisogno di qualcuno che in un attimo possa, politicamente e operativamente, prendere delle decisioni: il Presidente del Consiglio dal punto di vista politico attraverso la linea di condotta di

comando e controllo del Servizio di informazione per la sicurezza della Repubblica, e un'agenzia anche concettualmente moderna rispetto ai servizi italiani.

Abbiamo avuto servizi che per molti anni erano sempre un po' gelosi delle proprie prerogative. Credo che la situazione internazionale imponga di compiere passi – l'abbiamo fatto, perché credo che il CASA (Comitato di analisi strategica antiterrorismo) ne sia uno straordinario esempio – concettuali incredibili per gli standard europei. Gli europei non hanno neanche un'idea di quanto noi siamo avanti rispetto a loro. Credo che essere partiti molto più tardi di tutti gli altri sia stato, da una parte, un problema, perché mentre parliamo giovani dei vostri collegi perdono lavoro per l'inazione italiana; ma, dall'altra parte, abbiamo e avete la grande possibilità di imparare gratis – da genovese questo è importante – dagli errori degli altri Paesi e applicare un modello già da subito ideale e funzionale. Lo si può fare.

ANGELO TOFALO. Vorrei formulare una domanda, al di là delle considerazioni generiche. Su tavoli europei giustamente ci si sta ponendo il problema e si sta discutendo di normalizzare l'ambito della *cyber-offence*, che anche lei ha richiamato. Subisco un attacco da un'organizzazione, da attivisti, da un Governo: è guerra ? È come un attacco fisico ? Rispondo ? Siamo in guerra ? La direzione sembra essere questa, giustamente.

Vorrei semplicemente conoscere la sua opinione relativamente all'*attribution*. Il nodo è costituito dal dilemma tecnico. Se ricevo degli attacchi informatici, almeno a oggi, con gli strumenti che abbiamo, posso individuare un attacco di tipo cinese o statunitense, ma non lo so con certezza al cento per cento. Su questo punto qual è il suo pensiero ?

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Grazie all'indulgenza del presidente, in altre occasioni sono stato vostro ospite e ho affrontato un tema che mi preoccupava molto. Il vero problema è l'utilizzo di mezzi convenzionali gestiti da una politica non convenzionale.

Se, ad esempio, un Paese del Medioriente, che ha carri armati, aerei, sommergibili e navi, venisse guidato da gruppo dirigente che ha una visione diversa, e quindi non è convenzionale, non è statuale, avremmo un utilizzo di strumenti convenzionali con politiche terroristiche. Questo funziona, naturalmente, anche nel mondo virtuale, non soltanto nel mondo reale.

Lei ha ragione, il problema dell'*attribution* è fondamentale, ma credo che sia impossibile oramai dividere in maniera manichea tra il mondo reale e il mondo virtuale. Lo dico perché i danni che si possono fare nel mondo virtuale – parlavamo prima dell'esempio stupido, che mi perdonerà, del telefonino – possono ripercuotersi, anzi si ripercuotono in maniera anche amplificata nel mondo reale.

Cito un ultimo esempio, terribile, ma che dice qual è il futuro. Un ragazzino di 15 anni si è suicidato perché la ragazzina ha cancellato il suo contatto da *Facebook*. Avrà avuto tutti i problemi del mondo, nessuno lo discute, poi vedremo le famiglie, la storia e così via, ma non ci sono dubbi: per il futuro il mondo virtuale sarà un mondo nel quale le nuove generazioni interagiranno molto di più che nel mondo vero. Quelli del virtuale saranno, quindi, danni veri.

Abbiamo due tipi di problemi, onorevole Tofalo. Il primo è che le agenzie di *intelligence* degli alleati fanno *intelligence* su di noi, e quindi una parte delle risorse che potrebbero servire per combattere i comuni avversari sono, invece, usate per spiare gli amici, ma questo si è sempre fatto. Lei ha figli ? Io neanche, che io sappia, ma posso dirle che, quando amici che hanno figlie in età adolescente passando per il corridoio vedono la porta della stanza della figlia aperta e, incidentalmente, il diario sul tavolo, anche se è la figlia, i padri vanno a fare *intelligence*, e pure in profondità, spesso scoprendo cose che non avrebbero voluto scoprire.

Altro è, quindi, l'*intelligence* e lo spionaggio che fanno gli amici, tenendo conto che nel mondo dell'*intelligence* non ci sono

amici, ma temporanei compagni di viaggio; altro sono le attività offensive di penetrazione, di furto, di influenza, di ingerenza di Nazioni non amiche nei confronti nostri e dei nostri alleati.

Quelli non possono non essere considerati atti offensivi per un'unica ragione: se li consideriamo peccati e non reati, di fatto continuiamo a mantenere la porta aperta allo *shopping* dentro casa nostra, quindi quelle devono essere, secondo me, considerate operazioni offensive. E alle operazioni offensive si risponde in maniera molto netta, molto chiara. Spero di aver risposto.

DANIELE MARANTELLI. Io ho fatto l'alpino in Alto Adige quarant'anni fa, e nonostante ciò, anzi forse proprio per questo, ho ascoltato con vivo interesse le considerazioni del professor Margelletti. Attraverso le mie categorie un po' artigianali, ho l'impressione che non sia così certo che i settant'anni che abbiamo conosciuto in Europa di pace, con la drammatica eccezione dei Balcani, possano riprodursi per i prossimi settanta, andando a uno sguardo a pendolo della storia del mondo. Del resto, ci accorgiamo di come i confini di taluni Stati siano ormai cose virtuali, labili. Parlo di Stati che stanno davanti all'uscio di casa nostra.

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Chiedo scusa, pensi che io addirittura non li considero neanche più Stati. Pensi come siamo messi.

DANIELE MARANTELLI. La sproporzione clamorosa di risorse destinate sul tema tra l'Italia e Paesi che possiamo chiamare amici è – lei diceva, se ho capito bene – colmabile anche con iniziative artigianali. La ragione della mia curiosità sta nel fatto che noi spingiamo sempre più perché l'Europa abbia una politica estera, una politica di difesa e una politica della ricerca comune.

Credo, invece, che giustamente nella proposta di agenzia che ha illustrato, se ho colto bene, abbia sottolineato come queste dovrebbero essere essenzialmente nazionali, solo nazionali. Naturalmente, ne capisco il senso, ma come conciliare queste esigenze, entrambe giuste ? Può sembrare una contraddizione insanabile, insuperabile, ma invece credo che si debba trovare una strada. Mi sembra che entrambe le cose abbiano una loro consistenza. Le sarei grato se riuscisse a darmi una risposta su questo punto.

GIANLUCA FUSILLI. Evito le considerazioni dei colleghi, alle quali mi associo, circa il ringraziamento e l'interesse per il contributo del professor Margelletti. Mi collego a quanto diceva il collega Marantelli, anche perché in sostanza era quello che mi aveva colpito un po' di più della sua relazione, ovvero alla sottolineatura di quanto quest'agenzia, questa nuova infrastruttura dovesse avere un carattere meramente nazionale. La logica è quella di comprendere, e lo ha spiegato in maniera molto chiara, quanto la minaccia nell'ambiente virtuale possa avere conseguenze dirette sulla vita reale ed economica degli Stati, dei Paesi e dei singoli individui.

Ancora di più la precisazione si lega a quella del collega Marantelli perché è noto a tutti noi nell'esperienza quotidiana quanto un *default*, o comunque una difficoltà economica di un Paese dell'Unione europea, si riverberi sull'economia di tutti gli altri in maniera pesante e significativa. La ricerca di un punto di equilibrio tra il tenersi strette le capacità nazionali, ma cercare anche un coordinamento minimo di difesa comune, scambiandosi anche delle esperienze, dovrebbe essere interesse di tutti. Mi interessa che specifichi un po' di più le ragioni della sua sottolineatura.

PRESIDENTE. Per quanto mi riguarda, questo è uno dei dati che è emerso con maggiore clamore e sorpresa nell'inizio di questa indagine conoscitiva. Ribadisco, c'è la verifica di un elemento sorprendente, in qualche modo anche clamoroso: in quella che è apparentemente la dimensione universale per eccellenza, la rete, improvvisamente tornano i confini. Mai come in questa vicenda è chiarissimo che ognuno si difende per conto suo, che non esistono amici, alleati né progetti condivisibili.

In questo senso, quanto pesa la non autosufficienza tecnologica in termini sia di *software* sia di *hardware* ? Si può proporre la creazione di un'agenzia nazionale, ma se siamo dipendenti dal punto di vista tecnologico e compriamo macchine o programmi, non siamo più solo noi. In quel preciso momento siamo accompagnati. Da questo punto di vista e da esperto, quale può essere un approccio che ci metta non dico in sicurezza, ma che ci aiuti a costruire un'indipendenza e un'autonomia un po' più vere ?

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Capirete che per dovere risponderò prima al presidente.

Se mi consentite una frase poco istituzionale, vorrei rendere l'idea di quanto pesi la non indipendenza con un'espressione: è un bagno di sangue. I sistemi che acquistiamo hanno delle *back door*. Non compriamo da un'azienda X, ma da Paesi.

Tutti voi conoscete l'importanza – e gli Stati Uniti ne hanno fatto una bandiera – dell'indipendenza di stampa, del diritto all'informazione. Dopo l'11 settembre su tutte le reti americane, in particolare sulla CNN, la realtà per eccellenza del mondo globalizzato delle informazioni, scomparvero tutte le notizie sulle Forze armate americane e sui relativi spostamenti. L'amministratore delegato disse che capiva che si voleva sapere se e dove si stavano spostando portaerei e così via, ma la realtà è che la CNN è una rete televisiva americana. *Google*, *Cisco* e potrei andare avanti per ore, pesano tantissimo. Ci vorrebbero decine e decine di anni per andare alla pari con investimenti che non siamo neanche in grado di immaginare.

Da qualche altra parte, però, possiamo mettere un confine, un paletto. E il paletto che io considero una sorta di limitazione danni è quello di avere un'organizzazione almeno funzionale. Se non abbiamo la tecnologia, ma contestualmente non sappiamo che cosa fare perché l'organizzazione si disperde in mille affluenti e non tre, siamo spazzati via.

Io sono un europeista convinto, e immagino anche lei, onorevole. Detto questo, io e lei e pochi altri possiamo andare in Cina a mangiare bambù come i panda, perché siamo animali in via d'estinzione. Io mi occupo di politica internazionale da almeno 25-30 chili fa; ero un ragazzo splendido e mi addolora dire che non c'è una singola volta in cui temi fondanti sulla politica estera europea siano presi collegialmente.

Diverso tempo fa, il presidente mi invitò qui, proprio in Commissione difesa, a parlare dei *Battlegroup* europei e io dissi che erano tutti da chiudere, per la semplice ragione che non ne utilizzavamo nemmeno uno, non sono mai stati utilizzati, non verranno mai utilizzati e spendiamo soltanto dei soldi. A distanza di tempo, continuiamo a non utilizzare un singolo *Battlegroup* europeo; non solo noi italiani, ma anche gli altri.

Dobbiamo crederci, però, nell'Europa. I sogni sono gratis, da genovese lo sostengo. Devo dirle, quindi, che dobbiamo mettere a sistema gli intenti, ma non necessariamente gli strumenti. Quando sento parlare di Forze armate o di servizi segreti europei, sorrido. Le Forze armate o i servizi segreti sono, ad esempio, anche se non gli unici, due strumenti di sovranità nazionale. Per avere le Forze armate europee occorre avere gli Stati Uniti d'Europa o l'Europa oppure diventeremo tutti tedeschi. Lo stesso discorso vale per i servizi di informazione e sicurezza. Puoi mettere a confronto e a sistema le informazioni, ma non le fonti, per chi come me è appassionato di James Bond.

Perché le dico che deve essere assolutamente nazionale e non deve parlare con nessuno ? Perché deve essere una realtà che in ambito pubblico e privato, come dicevo, bollina e certifica l'*hardware* e il *software* da utilizzare. Inoltre deve essere l'unica realtà all'interno della quale si sa quali siano le capacità nazionali.

Vuole una risposta più dotta alla domanda che ha posto ? Ovviamente, non sono così capace di rispondere. Le consiglio di leggere uno splendido libro di Ken Follett o di vedere un bellissimo film con Sean Connery, la *Casa Russia*. All'interno di questo film, Sean Connery, un agente improv-

visato, dà a un russo un plico con mille domande che i servizi segreti inglesi e americani avevano preparato perché questo evidentemente aveva le risposte. Gli americani sperano che siano fornite tutte le risposte. Gli inglesi, che sono quelli che sanno fare l'*intelligence* sul serio, dicono che è un disastro se è una trappola, come in effetti era: attraverso le domande che si formulano, infatti, si capisce quanto sa chi le fa.

È la ragione per la quale non possiamo mettere a sistema le nostre capacità, perché dimostreremmo quanto sia nudo il re. Gli altri capirebbero così il nostro livello di capacità, aspetterebbero l'ora giusta per far alzare la marea e, quindi, passare dall'altra parte. Per questa ragione di sovranità nazionale, non di antieuropeismo, alcune caratteristiche e alcune capacità devono esclusivamente rimanere in ambito nazionale.

Lei mi poneva una domanda provocatoria in qualche senso, anche sulle risorse. Parliamo di risorse. Veda, a me non preoccupa quanto spendiamo. Sono molto più preoccupato di quanto buttiamo via e sprechiamo. Non possiamo fare la gara con gli inglesi, perché mettono 3 miliardi di sterline, con gli americani che mettono 200 miliardi di dollari, o coi tedeschi, che mettono 1 miliardo di euro.

Non posso, oggettivamente, come analista politico venire qui e chiedere a voi di trovare delle risorse economiche se queste non ci sono. Si tenga conto, peraltro, che quelli per la sicurezza sono soldi maledetti, perché la comunità non riesce a percepirli. Se non sta succedendo qualcosa, perché devo investire in sicurezza ? Contestualmente, non sta succedendo qualcosa perché ho investito in sicurezza. Mi rendo conto che spendere sull'invisibile è politicamente poco spendibile. Sono umanamente molto vicino a voi.

Per questo non sono qui per farvi il discorso ideale di tirare fuori 1,5 miliardi di euro per spenderli. Questo Paese ha tante priorità. Facciamo la guerra al cento per cento al terrorismo, alla mafia, alla disoccupazione e alla malasanità. Ricordo che abbiamo un cento per cento solo.

Quello che vi chiedo come analista politico non è di spendere di più, ma di spendere meglio. Possiamo considerare questa una goliardata e chiuderla qui. Di fronte a 12 nuclei in 15 tavoli, 16 specializzazioni, 4 commissioni, 3 servizi segreti e 5 amministratori di condominio, non ce lo possiamo permettere. Abbiamo pochi soldi: spendiamoli bene. Di più non si può oggettivamente fare.

Trovare soldi forse è impossibile, onorevole, spenderli bene no. Spero di aver risposto alla sua domanda.

MASSIMO ARTINI. Innanzitutto, mi scuso con il professor Margelletti, ma avevo un *question time* in Assemblea e non ho potuto seguire tutta l'audizione. Se dovessi fare una domanda già posta, avvertitemi.

Nella risposta che ho sentito già ritrovo molti spunti, in particolare quello della sovranità, che è quello cardine. Credo che il passaggio che ne derivi sia fondamentale.

Prima ho sentito parlare in maniera molto favorevole della struttura creata dalla Gran Bretagna relativamente all'approccio sulla *cyber*. Concordo con lei che la semplificazione di quella lastrina è anche troppo gentile rispetto a quella della struttura definita dal decreto del presidente del Consiglio del 2013 che per me è di una complessità estrema che viene salvata dal fatto che nella realtà le amministrazioni si adeguano. A livello normativo, però, siamo effettivamente davanti a qualcosa che genera imbarazzo alla vista.

Vorrei sapere cosa ne pensate sull'eventualità di implementare un'agenzia completamente svincolata dalla parte servizi, in particolare un'autorità delegata che riguardi esclusivamente il mondo della *cyber*, che copra tutti i settori, nel rispetto della nostra Costituzione, ma che parta dalla difesa, dal crimine e anche dal *warfare*, argomento eventualmente trattato ma non normato ancora in questo Paese.

Mi riferisco alla definizione di un'agenzia che abbia la possibilità di definire direttive, di gestire passaggi non dico autonomi, ma che sia comunque svincolata dalla parte esclusiva dei servizi. Per il mio modo di vedere, il mondo cibernetico non è solo servizi, è sovranità industriale, è

industria, è collaborazione privato-pubblico ed è un mondo completamente diverso. Su questo vorrei una sua valutazione.

ANDREA MARGELLETTI, *Presidente del Centro Studi Internazionali* (Ce.S.I.). Prima di tutto, dovremmo avere il coraggio, come lei ha avuto, ma l'abbiamo avuto tutti, di dire che non c'è solo il *cyber-defence*, ma anche il *cyber-offence*. Discutere di una cosa senza l'altra è inutile. Abbiamo detto che è necessaria una rapidissima implementazione del comando cibernetico di interforze per fare quel tipo di attività, che non è la protezione della rete della Difesa per evitare che si leggano le *e-mail* degli ammiragli, ma una cosa completamente diversa.

Dall'altra parte, sono fortemente perplesso sull'avere un'agenzia che si occupi di *cyber* svincolata, fuori dall'architettura dei servizi di informazione e sicurezza. Dicevo prima – mi perdoneranno i suoi colleghi se mi ripeto – che ritengo che le Forze dell'ordine debbano mantenere una loro capacità per le attività operative, come le due agenzie, AISI e AISE, che devono mantenere una capacità *cyber*. Stanno facendo attività su questo, hanno bisogno dei tempi, perché la velocità è tutto oramai.

Una realtà importante che parli con i grandi gruppi industriali, ma anche con la piccola e media impresa – altrimenti si protegge il grande gruppo industriale, ma la filiera non esiste più – non può non essere rapida. Inoltre deve avere un responsabile politico molto netto e forte, che abbia un controllo parlamentare importante. Per questo immaginavo un'agenzia all'interno dell'architettura dei servizi, assolutamente pari e sotto il DIS: perché ?

Il mio timore – anche per questo chiedo l'indulgenza del presidente e vostra se mi rivolgo in maniera poco ortodossa, ma voglio essere molto chiaro – è che nell'ipotesi questa diventasse una sorta di *authority* esterna, ci sia l'assalto alla diligenza e che, nella compartimentazione dei vari ministeri che vogliono esserne parte, quest'*authority* perda la sua capacità di essere presente su tutto il territorio nazionale, isole comprese, 24 ore su 24 per 365 giorni all'anno, con quelle capacità di proiezione, protezione e invasività, quando è necessario, che non può avere una sorta di *authority*.

Abbiamo bisogno di una struttura che sia dove ci sia qualcuno che se ne prenda pienamente le responsabilità, perché stiamo parlando di entrare nelle vite delle persone, non soltanto di proteggerle. Ci vuole qualche autorità che si assuma la responsabilità, e non vedo responsabilità più alta di quella del Presidente del Consiglio dei ministri. Perfetto.

Nel momento in cui in maniera invisibile violo la *privacy*, l'identità, i fondi, la famiglia, gli studi, gli *hobby* e i piaceri del dottor Massimo Artini, ho bisogno che ci sia un controllo parlamentare stringente. Stiamo parlando di cambiare la vita delle persone e addirittura di poterle inquinare se questo è utile per la sicurezza nazionale.

Le Forze dell'ordine continuino a fare le loro attività, ma questa è una realtà talmente importante che non fa solo *intelligence*. Questa parte c'è, la fa, ma deve essere anche la componente che va presso le aziende dicendo che non sono sicure, che devono regolarsi in un certo modo per gli standard nazionali, che sono uno o dieci tipi di *software*, che però noi certifichiamo. Diversamente, onorevole, è la giungla, che conoscete molto meglio di me.

Questo tipo di autorevolezza è data dalla Presidenza del Consiglio, dal controllo parlamentare e, naturalmente, dalla certezza che si sta parlando con dei professionisti che lo fanno tutti i giorni, nell'ambito dei servizi di informazione e sicurezza.

Altro è la *cyber-offence*, che dovremmo sviluppare tantissimo e che, invece, è una competenza militare. Ho anche detto che abbiamo un tavolo tecnico quotidiano, il CISR tecnico, una sorta di CASA, che potrebbe essere un ulteriore passo in più per implementare. Di questo, secondo me, abbiamo bisogno. Veramente il rischio è che, di fronte a *budget* importanti che possono arrivare, a interessi vari, si trasformi in qualcosa che non deve essere.

PRESIDENTE. Ringraziamo ancora il professore Margelletti per gli spunti che ci

ha offerto, per le informazioni e per le riflessioni che ha posto sul tavolo. Saranno sicuramente molto utili per il seguito del nostro approfondimento nell'ambito di questa indagine conoscitiva.

Dichiaro conclusa l'audizione.

**Audizione dell'avvocato Stefano Mele, specializzato in Diritto delle tecnologie, *privacy* e sicurezza delle informazioni, consulente in materia di *cyber-security*, *cyber-intelligence*, *cyber-terrorism* e *cyber-warfare*.**

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico l'audizione dell'avvocato Stefano Mele, esperto in diritto delle tecnologie, *privacy* e sicurezza delle informazioni, consulente in materia di *cyber-security*, *cyber-intelligence*, *cyber-terrorism* e *cyber-warfare*.

Saluto e do il benvenuto all'avvocato Mele, che ringrazio per la sua presenza. Come sempre, dopo la relazione del nostro ospite i colleghi potranno formulare domande e osservazioni, cui l'avvocato risponderà alla fine.

STEFANO MELE, *Specializzato in Diritto delle tecnologie, privacy e sicurezza delle informazioni, consulente in materia di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare*. Grazie mille, presidente, per l'invito. Anzitutto, è per me davvero un grandissimo onore essere qui e parlare di un argomento che reputo molto interessante e attuale.

Se mi è permessa una digressione, dobbiamo a mio avviso cominciare riflettendo sul punto di partenza di questo genere di attività, cioè delle attività di *cyber-warfare* da parte degli Stati. Dobbiamo anzitutto cominciare a ricordare che, per esempio, nel 2007, nove anni fa, prima di bombardare una centrale di arricchimento dell'uranio a Damasco – è un'informazione pubblica – Israele ha pensato di penetrare i sistemi informatici di controllo dello spazio aereo siriano, sistemi ovviamente di matrice russa, di disattivarli senza spegnerli, di far alzare in volo i propri cacciabombardieri, di passare sul territorio e bombardare. Ovviamente, lo Stato si è accorto dell'attacco cinetico, quindi con un bombardamento, dopo che il primo missile ha colpito il bersaglio. Siamo nel 2007.

Nel 2010, ancora una volta Israele e Stati Uniti d'America, così riportano i libri, creano un *malware* capace di spaccare fisicamente una centrale di arricchimento dell'uranio, questa volta in Iran, a Natanz per essere precisi. Riescono attraverso un « semplice » *software* a passare da un mero danno virtuale al danno fisico facendo andare le ventole di raffreddamento delle centrali di arricchimento dell'uranio a Natanz, in Iran, in extrarotazione per giorni, fino a farle spaccare. La CIA stimò un rallentamento della produzione in alcuni casi, ma in altri anche l'impossibilità, per due anni, di arricchire l'uranio in quelle centrali. Siamo nel 2010, sei anni fa.

Già solo cominciando a ragionare in questo senso, mi sembra molto interessante pensare a come già da tempo alcuni Stati si siano attivati per attacchi di *cyber-warfare*, cioè di conflittualità attraverso l'utilizzo delle tecnologie nel e attraverso il *cyber*-spazio. Non amo molto il termine *cyber-war*, perché da giurista a mio avviso ci sono delle norme che specificano quando è guerra: semplificando, devono esserci dei morti o dei danni fisicamente rilevabili su strutture del Paese colpito. Fino a questo momento, forse solo Stuxnet potrebbe essere visto come un'arma, come una cosiddetta *cyber*-arma, e quindi avere come conseguenza tutto quello che tra un po' cercherò di spiegare.

Sappiamo perfettamente che si dice che a dicembre del 2015 – lo vedremo tra un po' – un Governo di una delle maggiori potenze a livello globale sia riuscito, attraverso ancora una volta un attacco informatico, a interrompere l'erogazione dell'energia elettrica in una grossa fetta occidentale del territorio ucraino. Evidentemente, il problema è molto più che atteso. È addirittura un problema che a mio avviso nasce già nel 2007, nel 2010, per cui è da un po' di tempo che stiamo ragionando su questo genere di attività.

Ribadisco che non mi piace parlare di *cyber-war*, ma nel *cyber*-spazio sicuramente le tecnologie per scopi militari hanno assunto nella pratica il ruolo di facilitatore di attacchi cinetici attraverso i domìni tradizionali di aria, terra, mare e spazio. Non soltanto alcuni Stati hanno già iniziato le attività, nel 2007, nel 2010 e nell'altro caso che ho citato, ma ormai cominciano anche a inserirlo palesemente all'interno delle loro strategie.

Non si parla più soltanto nelle strategie dei Governi di *active cyber-defence*, di una difesa attiva che cerca di comprendere se per caso ci siano elementi per cercare di recuperare il vero attaccante. Qui parliamo di un vero e proprio sviluppo di capacità offensive nel *cyber*-spazio, e viene detto chiaramente. Lo dicono chiaramente, per esempio, gli Stati Uniti in un documento pubblico, rilasciato pubblicamente nel 2013: il Cyberspace Operations, del Pentagono, quindi dei militari americani.

All'interno di questo documento viene formalmente riconosciuto l'impiego da parte degli Stati Uniti delle attività militari offensive. Per quale scopo ? Per proiettare la forza nel e attraverso il *cyber*-spazio al fine di « degradare, danneggiare o distruggere l'accesso, il funzionamento o la disponibilità delle capacità di un bersaglio ad un livello e per un periodo di tempo determinato ». Definiscono anche cosa sono, e qui le riporto, le *offensive cyber operations*: sono le attività volte « a controllare o modificare le informazioni, i sistemi informatici o le reti dell'avversario ».

È vero che il Governo all'interno di questa *policy* dice che deve essere autorizzata singolarmente da Obama ogni operazione militare di questo genere e che l'obiettivo deve essere militare, ma voi mi insegnate che molte infrastrutture tecnologiche che servono ai militari sono civili, quindi potrebbe essere anche molto interessante vedere nella pratica come effettivamente si potrebbe colpire, se possibile, soltanto obiettivi militari.

Del resto, tornando per esempio al famosissimo caso di Stuxnet, essendo un *malware* ed essendo stato programmato per una serie di comandi e per colpire una serie di obiettivi – tutti i sistemi informatici della Siemens che avevano quei problemi di sicurezza – ha colpito gli Stati Uniti stessi. Si è, infatti, propagato su *Internet* e ha fatto quello per cui era programmato, cioè cercare tutti i sistemi della Siemens che avevano quei problemi: una volta trovati, ha attivato il *payload* di « arma di attacco ».

È sicuramente interessante vedere negli effetti che cosa fino adesso si è riuscito a fare, ma lo hanno già fatto e ormai si è sempre meno timidi da parte di un numero sempre maggiore di Stati, prima di tutto gli Stati Uniti, ma ancora la Cina. Il 31 dicembre 2015, la Central Military Commission cinese ha pubblicamente annunciato di aver completato una sostanziale riforma organizzativa della People's Liberation Army, ovvero le Forze armate cinesi, creando tre nuovi organismi: l'Army Leading Organ, la Rocket Force e la Strategic Support Force.

Tra le tre, la Strategy Support Force è quella che ci interessa di più dal punto di vista della *cyber-security*, perché al suo interno hanno creato a loro volta tre diverse ramificazioni. Che cosa hanno fatto, di molto interessante ? È un *trend* che era già presente negli Stati Uniti e che presto secondo me attueranno moltissimi altri Stati: hanno dapprima inserito sotto la medesima linea di comando operazioni militari e di *intelligence* sia difensive sia offensive, ovviamente attraverso il *cyber*-spazio; hanno poi creato una seconda ramificazione che si occupa di operazioni militari condotte nello spazio, altro problema, come già sapete, su cui si sta andando sempre più velocemente; infine, la terza ramificazione è quella parte di *electronic warfare*.

Hanno, quindi, accentrato all'interno di un'unica linea di comando, di un unico punto anche geografico, tutto questo. Perché ? Perché le tecnologie comportano una necessità di risposta e di valutazione temporale dell'attacco molto immediata. È un lasso di tempo su cui non siamo abituati a ragionare e su cui, probabilmente, nessun essere umano può ragionare.

Non è un missile a lungo raggio, che giustamente quando fu creato accorciava le tempistiche, perché prima si ragionava con tempistiche di guerra completamente differenti. Quando furono creati i missili a lungo raggio si era cominciato a ragionare nell'arco dei 10-15 minuti che il missile ci avrebbe messo per arrivare da una parte all'altra del globo. Oggi ci fa ridere questo spazio temporale, perché siamo abituati a ragionare con le tecnologie su questo spazio.

In questo caso, la materia è molto giovane e ancora non riusciamo a ragionare in termini di millisecondi. Dobbiamo concentrarci nella creazione di *software* che difendano automaticamente con delle regole di ingaggio minime già inserite al loro interno. È molto interessante questo *trend*, ma sappiamo che Stati Uniti e Cina sono « dall'altra parte del mondo », anche se gli Stati Uniti molto meno di quello che si può pensare, e che sono potenze a livello globale, quindi sono anche *cyber*-potenze, se mi passate l'espressione sicuramente poco tecnica.

In realtà, anche i Paesi europei si stanno spingendo verso le operazioni offensive. Il Regno Unito, per esempio, il 23 novembre 2015, ha emanato la nuova Strategic Defence and Security Review, come si sa uno dei documenti più rilevanti per comprendere la postura strategico-militare del Regno Unito. Che cosa hanno scritto le Forze armate inglesi ? Hanno scritto che conseguiranno capacità militari offensive avanzate nel e attraverso il *cyber*-spazio.

Io sono un avvocato e, se qualcuno scrive di capacità militari offensive avanzate, mi fa comprendere che quelle non avanzate già le ha, ma posso sbagliare. In ogni caso, è indicativo che da qui – dalla fine del 2015, inizio 2016 – ai prossimi cinque anni, persino un Paese europeo come il Regno Unito sta sviluppando capacità militari offensive attraverso il *cyber*-spazio. Siamo addirittura venuti a conoscenza di un *National Offensive Cyber Programme* inserito sempre in questa Strategic Defence and Security Review. Ancora una volta, da chi è gestito questo *National Offensive Cyber Programme* del Regno Unito ? In *partnership* tra il Ministero della difesa e i servizi. Ancora una volta si accentrano capacità militari e capacità di *intelligence* sotto una medesima linea di comando.

Potrei parlarle della Danimarca, che con mio sommo stupore proprio recentemente ha tirato fuori un documento all'interno del quale si dice che creeranno una scuola per fare attività militari offensive e di *intelligence* attraverso il *cyber*-spazio. Ci sono notizie relative all'Australia della scorsa settimana. Si stanno tutti muovendo in questa direzione.

Se ciò è vero, come io reputo che sia, ragionare sulle norme, su che cosa possiamo fare in caso di un attacco informatico e se possiamo reagire a un attacco informatico con un attacco informatico o con un attacco cinetico – lo vedremo magari successivamente – credo che sia un elemento non da poco. Si sente ripetere all'infinito che mancano norme di diritto internazionale specifiche per questo genere di problematica.

È vero, non lo nascondo, ma bisogna ricordarsi che, per quanto riguarda il diritto internazionale – ovviamente, di diritto internazionale dobbiamo parlare quando ci sono due Stati che si fronteggiano – la clausola Martens, comparsa addirittura nella IV Convenzione dell'Aia e poi ripresa nelle quattro convenzioni di Ginevra del 1949, già ci dà la possibilità di estendere gli istituti che conosciamo e di cercare di comprendere e verificare se possiamo adattarli alle nuove situazioni. Si può fare, possiamo prendere le norme consuetudinarie che conosciamo e cercare di vedere se effettivamente si adattino o meno al diritto internazionale.

Peraltro, come normalmente non viene fuori, già dal 2013 il gruppo di esperti delle Nazioni Unite che si occupa di questioni legate all'*information and communications technology* in ottica di *international security* aveva detto che il diritto internazionale vigente si applica anche all'interno del dominio cibernetico, così come avevano specificato i concetti tradizionali di sovranità statale.

Dato che, evidentemente, non era abbastanza chiaro, nella riunione e nel *report*

del 2015, sempre il medesimo gruppo è andato un po' più in maniera chiara a esplicitare alcuni concetti, che reputo veramente molto interessanti in questo dibattito. Hanno convenuto e messo all'interno del loro *report* che gli Stati esercitano la loro giurisdizione sulle infrastrutture informatiche situate sul loro territorio, cioè la competenza territoriale di uno Stato non viene meno. È un elemento da un punto di vista giuridico molto interessante.

Ancora, nel successivo punto, all'interno di questo *report* viene specificato che nell'utilizzo degli strumenti informatici gli Stati devono rispettare, oltre agli altri princìpi di diritto internazionale, quello dell'inviolabilità della sovranità territoriale altrui, della parità tra le diverse sovranità territoriali, dell'assestamento dei conflitti mediante mezzi pacifici e, soprattutto, la non ingerenza nelle questioni interne di altri Stati. Sono i princìpi fondamentali del diritto internazionale consuetudinario che conosciamo.

Specificano anche – lo sottolineo – che i vincoli legali internazionali già esistenti sono applicabili anche all'utilizzo da parte degli Stati di strumenti informatici. Dobbiamo non solo applicare questi, ma ricordarci anche la protezione dei diritti umani e delle libertà fondamentali. Mi sembra molto chiaro che le norme di diritto internazionale vigente consuetudinario possano e debbano trovare applicazione già nella loro formulazione odierna.

Il gruppo all'interno del *report* continua nell'elencazione di alcuni altri elementi. Bisogna, ovviamente, guardare anche ai princìpi internazionali di umanità, necessità, proporzionalità e distinzione, che sono elementi fondamentali. Soprattutto, gli Stati non possono commettere, rimarca il gruppo di esperti, atti internazionalmente illeciti mediante strumenti informatici, neanche attraverso deleghe a terze parti, quindi nemmeno – qui si colma un problema nato da un po' di tempo – dando in carico a soggetti terzi, a gruppi criminali o a soggetti che fanno questo di lavoro, e ce ne sono, l'operazione militare contro uno Stato.

Qualora venga evidenziata una tale situazione, la responsabilità sarà sempre dello Stato che ha dato mandato a questi gruppi « civili » o paracivili di fare questo genere di attività. C'è già. È nel diritto internazionale. Non dobbiamo inventarci niente. Inoltre, il territorio non deve essere utilizzato da attori non statali al fine di commettere tali atti.

L'ultimo punto è, invece, un po' forse una risposta agli Stati Uniti d'America, che sempre più stanno pubblicamente – è una strategia di deterrenza – individuando persone e soggetti fisici dicendo nome e cognome di chi ha provato ad attaccare i loro sistemi informatici. L'hanno fatto l'anno scorso più volte, un paio di volte nei confronti dei cinesi. Forse a questo è legato il fatto che il gruppo nel 2015 ha anche convenuto che non bastano semplicemente degli indizi, ma se uno Stato accusa un altro Governo, deve portare delle prove.

Tuttavia la tendenza è questa perché gli Stati Uniti – da un po' di tempo, l'hanno fatto proprio di recente, il mese scorso – hanno specificamente indiziato degli iraniani di attività *cyber* contro i propri interessi. Addirittura, avevano commesso un attacco a una diga a New York, che fortunatamente non avevano aperto pur potendo, perché avrebbe inondato la città e ucciso delle persone. Questo è il livello su cui stiamo ragionando, il livello di minacce, di pericolosità di azioni compiute nel e attraverso il *cyber*-spazio in questo momento, un livello altissimo. Dunque, nel caso in cui un Governo debba o intenda puntare il dito contro un altro, dovrà portare delle specifiche prove.

A mio avviso, si possono evidenziare alcuni elementi interessanti nella prassi degli Stati in ordine all'applicazione delle norme riguardanti lo *ius ad bellum*, contenute soprattutto nella Carta delle Nazioni Unite. Queste norme possono essere applicate alle operazioni informatiche. Per questioni di tempo, rifletterò in particolare su due norme che mi sono sembrate più interessanti in questa fase, e soprattutto con il tema di capire se sia possibile la reazione legittima di uno Stato a un attacco informatico.

La prima da prendere in considerazione è sicuramente l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite. Lo conosciamo tutti: « Tutti gli Stati membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite ».

Quest'articolo è genericamente già ritenuto applicabile ed essenziale alle operazioni informatiche, ma crea dei problemi non da poco, che vorrei porre in questo momento per verificare – la mia estrazione è quella di fare l'avvocato, e quindi normalmente devo dare delle soluzioni – se possono essere risolvibili o sono già stati risolti, almeno dal mio punto di vista.

Per ritenere applicabile l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite, occorrono tre elementi fondamentali: il primo è che la condotta sia imputabile a uno Stato, in quanto la norma non si riferisce a individui privati o a gruppi armati; il secondo elemento è che l'azione possa essere classificata come una minaccia o un utilizzo della forza; infine, il terzo è che ciò avvenga nell'ambito delle relazioni internazionali. L'imputabilità a uno Stato è un punto a mio avviso prettamente tecnico, tecnologico. La risposta a questa domanda deve essere data dai tecnici, che devono trovare con attività di *computer forensics*, per esprimersi con un linguaggio tecnico, o di indagine, se usiamo un'espressione più generale, effettivamente chi abbia compiuto questo genere di attacco.

Da un punto di vista normativo, in realtà l'imputabilità di uno Stato può essere rintracciata. L'International Law Commission da tempo ha stilato un progetto di articoli sulla responsabilità degli Stati, approvato dall'Assemblea generale, che quindi possiamo considerare *ius cogens*, stabilendo quando è possibile da un punto di vista giuridico attraverso specifici criteri attribuire una condotta a uno Stato.

Per esempio, l'articolo 4 di tale progetto di articoli sulla responsabilità degli Stati stabilisce che il comportamento di un organo statale sarà considerato come un atto dello Stato ai sensi del diritto internazionale sia che tale organo eserciti funzioni legislative, esecutive, giudiziarie o qualsiasi altro genere di funzioni, o qualsiasi posizione abbia nell'organizzazione dello Stato, e quale che sia la sua natura come organo del Governo centrale o di unità territoriale dello Stato.

Peraltro, l'International Law Commission specifica che con il termine di organo non si deve intendere semplicemente un organo come lo intendiamo noi, ma è ricompresa anche qualsiasi persona che opera all'interno dell'organo. Questo amplia enormemente il ventaglio e la responsabilità dello Stato.

Il successivo articolo 5 disciplina anche casi in cui l'azione non sia perpetrata da un organo dello Stato, ma da un soggetto in qualche modo abilitato dal diritto di quello Stato a esercitare prerogative di Governo. È il caso in cui l'attaccante sia il membro di un ente parastatale, pubblico, semipubblico, di una società privatizzata autorizzata a esercitare questo genere di attività per conto del Governo.

Non solo, quindi, se il Governo lo fa come tale o attraverso i suoi uomini, ma anche nel caso in cui lo dia a soggetti terzi o a soggetti abilitati dal diritto di quello Stato a fare questo genere di attività, comunque continueremo a poter dare la responsabilità a questo Stato.

L'articolo 11, ancora, ritiene che la condotta non attribuita a uno Stato ai sensi di tutti gli altri articoli precedenti – per brevità ho citato solo quelli che giudico più interessanti – può essere comunque considerata responsabilità di quello Stato qualora comunque quello Stato ne sia a conoscenza e l'addotti come un'attività propria. È proprio a questo che determinate condotte particolarmente aggressive di alcuni Stati potrebbero essere ricondotte.

Purtroppo, infatti, come dicevo precedentemente, quella del subappalto dell'operazione militare o di *intelligence* a soggetti terzi esterni al gruppo è una pratica che abbiamo riscontrato essere da un po' di tempo quella maggioritaria. Questo comporta una serie di problematiche da un punto di vista tecnico per il rintraccio del

soggetto. Si potrà « facilmente » rintracciare l'autore materiale dell'attacco, l'organizzazione, o da dove è venuto l'attacco informatico, ma se è una società privata per dimostrare il collegamento col Governo serve un livello di *intelligence* e di indagine decisamente superiore.

Le norme, però, ci sono. Addirittura, l'ultimo caso è quello in cui le operazioni militari provengano da strutture informatiche presenti sul territorio e non vedano alcun coinvolgimento dello Stato: anche in questo caso, se prendiamo il progetto di norme dell'International Law Commission, potremmo comunque rivalerci contro con lo Stato e quanto meno accusarlo di non aver adottato le necessarie misure preventive per impedire quell'azione. Imputare la condotta a uno Stato, purché si riesca a individuarlo da un punto di vista tecnico, a livello normativo non è così complicato.

È il secondo elemento che, invece, crea un po' più di problemi. Come dicevo prima, perché possa essere applicato l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite, l'azione deve poter essere classificata come un utilizzo della forza. Purtroppo, su questo secondo requisito non esiste nel diritto internazionale una definizione univoca di uso della forza. Un'azione informatica potrebbe essere classificata come tale, ma nel momento in cui la sua intensità e i suoi effetti siano paragonabili a quelli di un attacco armato. Questa almeno è la dottrina che si appoggia sul concetto di valutare la gravità degli effetti, la dottrina maggioritaria che abbiamo fino a questo momento e su cui probabilmente concordano praticamente quasi tutti gli Stati.

Perché, a mio avviso, è importante valutare la gravità degli effetti ? Perché toglie attività di spionaggio, di sabotaggio o meramente criminali, che non costituiscono un uso della forza, ma altro. Si concentra esclusivamente, in questo caso con certezza, su tutti quegli atti che abbiano come effetto quello di danneggiare infrastrutture fondamentali. Siamo sicuri o possiamo essere sicuri, sotto il punto di vista del diritto internazionale, al cento per cento che ci troviamo di fronte a un utilizzo della forza e, quindi, che quell'azione può essere classificata come uso della forza, nel momento in cui vediamo un danneggiamento a delle infrastrutture fondamentali. Questa è la sicurezza. Più avanti sulla legittima difesa vedremo la parte un po' meno sicura. In ogni caso, questo è lo stato dell'arte.

Il terzo elemento è che ciò avvenga nell'ambito delle relazioni internazionali. Questa è la parte più facile, perché con la terza condizione si sottolinea che non solo la minaccia deve provenire da uno Stato, ma implicitamente deve anche essere rivolta a un membro della comunità internazionale, cioè si deve ragionare appunto sul piano delle relazioni internazionali. Quando abbiamo questi tre elementi, allora possiamo con tranquillità richiamare l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite.

La seconda norma su cui pongo la vostra attenzione è quella sulla legittima difesa. L'articolo 51 della Carta delle Nazioni Unite è più che conosciuto, quindi non mi soffermerei sul contenuto testuale, ma sul ragionare su che cos'è la legittima difesa, che può essere definita come la possibilità per uno Stato di rispondere, se necessario, a un illegale uso della forza che corrisponde, ancora una volta, a un attacco armato.

La legittima difesa, in realtà, è considerata sia un diritto innato dello Stato sia un'eccezione al divieto di uso della forza. L'inclusione di questo nella Carta delle Nazioni Unite ha, a mio avviso, una duplice valenza. Da una parte, infatti, vuole riconoscere il preesistente diritto degli Stati – comunque, uno Stato ha il diritto di difendersi, al di là se fa parte o meno delle Nazioni Unite – ma, dall'altra, vuole porre le basi sulla possibilità di una legittima difesa collettiva, che ha visto, tra parentesi, nel 2014 l'estensione anche al *cyber*-spazio.

Sappiamo, infatti, che l'articolo 5 ha incluso anche il *cyber*-spazio, quindi un attacco informatico portato con i canoni che abbiamo analizzato fino a questo momento potrebbe comportare una reazione di tutto il blocco, perché c'è stata quest'estensione. Ancora una volta andiamo verso conflitti cinetici appoggiati e soprattutto facilitati dall'utilizzo di tecnologie e della

rete *Internet*. La possibilità è di una legittima difesa collettiva.

La Corte internazionale di giustizia ha, tuttavia, da tempo stabilito che l'articolo 51 si applica – è per questo che ci ho messo un po' di enfasi parlando – a qualsiasi uso della forza, indipendentemente dal mezzo utilizzato. Questo è il famoso caso Nicaragua. Di conseguenza, emerge chiaramente che in questo caso già abbiamo una norma che permette una legittima difesa anche in caso di attacco informatico. A mio avviso, quindi, le norme già ci sono. Devono soltanto essere ragionate e valutate.

Non abbiamo, però, una definizione universalmente accettata di attacco armato, come sapete meglio di me. C'è una serie di definizioni. Quella che riporto l'ho lasciata nel testo inglese proprio per evitare di intaccarne la *ratio* che c'è dietro. Si vede l'attacco armato come un uso della forza originato fuori dal territorio dello Stato che ne è l'obiettivo, che sale ben oltre il livello di un incidente di piccola scala o di un attacco armato isolato o di un'attività criminale, diretto contro lo Stato, il territorio, vessilli, aerei eccetera.

Prendendo questa definizione e riferendola allo strumento informatico, un attacco armato potrebbe consistere, a mio avviso, in un'operazione informatica diretta contro le infrastrutture fondamentali dello Stato qualora avesse le potenzialità di compromettere seriamente le capacità di svolgere le funzioni dello Stato bersaglio o possa minare la stabilità politica, economica e sociale dello Stato, anche senza che ci siano evidenti danni fisici.

Per qualificare, però, in questo momento un attacco armato attraverso strumenti informatici – ci tengo a precisarlo – per essere sicuri occorrono i danni, un livello superiore di danno visibile, ma stiamo andando proprio verso questo. Perché ?

Fondamentalmente, dobbiamo cominciare a ragionare in maniera completamente diversa quando pensiamo agli attacchi informatici o alle operazioni militari e ai danni che le operazioni militari nel e attraverso il *cyber*-spazio possono fare. In maniera molto sintetica, è molto difficile che un attacco informatico abbia come effetto diretto il danneggiamento, anzi non avviene mai. Un attacco informatico ha come primo effetto quello di manipolare il *software* che gestisce l'infrastruttura, militare o di Governo o quello che volete; come secondo effetto può avere quello di creare un danno a livello informatico; addirittura come terzo effetto può avere quello del danno fisico.

Dobbiamo, quindi, per forza ragionare pensando come tecnicamente avviene un attacco informatico e come tecnicamente un *malware* commette o si attiva e porta « a compimento » la sua operazione. Non è mai una pistola che spara e il proiettile uccide. Purtroppo, non è così. Dobbiamo necessariamente cominciare a ragionare anche in assenza di evidenti danni fisici.

Oltretutto, allo stato attuale, conosciamo un solo *malware* che ha prodotto danni fisici: Stuxnet. Poi magari ce ne saranno altri che non conosco, ma comunque a livello pubblico è così. Tutti gli altri fanno danni. Se spengo una centrale che eroga l'energia elettrica, come è avvenuto a dicembre dello scorso anno in una parte molto ampia, occidentale, dell'Ucraina, comunque come terzo affetto si riversa sul cittadino, sui soggetti che rimangono senza energia elettrica. Possono anche morire come ulteriore effetto. Senza energia elettrica posso rimanere al freddo e in inverno da quelle parti le temperature sono molto basse; posso non avere cibo, non scaldarmi e così via.

Se non cominciamo a ragionare anche in quest'ottica – sul piano del diritto internazionale, soprattutto gli Stati Uniti e altre Nazioni, stanno spingendo enormemente sotto questo punto di vista – lasciamo aperta la porta ad attività indisturbata di *cyber-warfare* da parte di Stati. E non possiamo permettercelo. Come dicevo all'inizio, abbiamo già dei casi dal 2007, poi quello di Stuxnet nel bombardamento israeliano a Damasco, poi Stuxnet nel 2010 e poi questa centrale ucraina, ma ce ne sono anche altre interessanti.

C'è il caso di Saudi Aramco, la più importante società di estrazione petrolifera dell'Arabia Saudita, che si è vista format-

tati oltre 30.000 *hard-disk* attraverso un *malware*, bloccata l'estrazione e la produzione con danni economici rilevantissimi per circa due settimane prima che tutto fosse rimesso a posto e che la centrale tornasse in funzione. Dobbiamo ragionare urgentemente sotto questo punto di vista e per questo ho accolto veramente con grande gioia non solo il vostro invito oggi, ma il fatto che mi abbiate invitato a parlare proprio di quest'argomento.

Concludendo, dobbiamo ricordarci che ci sono altri tre elementi perché si possa invocare la legittima difesa – non solo che ci sia un attacco armato, di cui abbiamo già parlato – e reagire. Il primo è sicuramente che la necessità dell'uso della forza presuppone un pericolo imminente e la mancanza di altre possibili soluzioni pacifiche. Quindi dobbiamo necessariamente stare per essere attaccati o sotto attacco.

C'è poi la proporzionalità, altro elemento molto interessante, che si riferisce alla necessità che le contromisure adottate dallo Stato che subisce l'attacco in virtù del diritto di legittima difesa non eccedano la misura necessaria per reprimere o respingere l'attacco. Qui una domanda potrebbe essere: il principio della proporzionalità significa che, se mi attaccano a livello informatico, devo rispondere a livello informatico e devo essere così bravo da controllare il mio attacco e raggiungere la stessa soglia di danno ?

No, il diritto internazionale, in casi non relativi al diritto internazionale applicato a questo genere di attività ma ad altre, ha già risposto che non è assolutamente necessario. Possiamo anche rispondere lecitamente da un punto di vista del diritto internazionale già oggi a un attacco informatico con un attacco cinetico. Non c'è nessun obbligo di rispondere con la stessa carta, per intenderci.

È chiaro che forse un attacco cinetico crea molti più danni rispetto a uno informatico, ma qui dobbiamo sempre ragionare su un attacco informatico che ci permette di attivare l'articolo 51 o l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite, ovvero su un attacco che crea rilevanti problemi a livello nazionale e sul territorio o addirittura dei danni fisici.

Nonostante ciò, dobbiamo ricordarci che, almeno dal mio punto di vista e almeno per le informazioni di cui dispongo, un attacco informatico non è mai, come dicono i militari, definitivo. Non è un missile che colpisce la centrale di arricchimento dell'uranio in Iran e a Damasco in Siria e la distrugge, e quindi bisogna ricostruirla da capo. Un attacco informatico, per quello che sappiamo fino a oggi, è un attacco che, come è successo con Stuxnet, ha bloccato in alcune centrali l'arricchimento dell'uranio per due anni, ma poi il pezzo si ricompra, lo si reinserisce.

Lo dico contro i miei interessi, per l'amor di Dio. Svolgendo questo genere di attività e essendo focalizzato su questo, non ho interesse a dirlo, ma dobbiamo ragionare su questo. Un attacco informatico non crea mai un danno definitivo, non è mai risolutore, almeno fino a questo momento.

Vengo all'ultimo elemento, l'immediatezza: per avere una reazione legittima da parte di uno Stato a un attacco informatico dobbiamo reagire o lo Stato soggetto all'attacco deve reagire nel minor tempo possibile, o comunque in un lasso di tempo ragionevole. Non possiamo subire l'attacco oggi e ricordarci tra due anni di fare una *retaliation*, dare una risposta. Questo mi sembra un principio sicuramente, soprattutto per chi fa la parte di diritto, abbastanza ovvio e logico.

In questo momento potrebbe essere, però, un problema piccolo, ma risolvibile. Allo stato attuale, anche gli Stati Uniti, come dicevo, che sono più avanti di tutti e che riescono già oggi, in questo momento, a dire che ad attaccare la diga a New York nel 2013 sono stati tre iraniani, con foto, nome e cognome, cosa fanno nella vita eccetera, hanno impiegato un arco di tempo sicuramente molto rilevante, dalla fine del 2013 agli inizi del 2016, che non permette nel caso di ricercare il criterio dell'immediatezza. È chiaro che col tempo andremo sempre più velocemente.

Mi sono permesso di portare questa vignetta che trovo molto interessante. Onestamente, non so se le storie di guerra del

futuro saranno così, cioè di un nonno che racconta ai suoi nipoti ricordando quella volta in cui erano all'interno di un *firewall* cinese, avevano delle *botnet* da una parte e dei *server* dall'altra, bruciati in una notte sola. Probabilmente, ci metteremo ancora molto tempo ad arrivare a questa situazione.

Quello che, però, voglio e spero di aver trasmesso è che gli altri Stati si stanno attrezzando e lo stanno facendo molto velocemente. Hanno già cominciato a muovere attacchi sin dal 2007; per gli Stati Uniti potremmo addirittura datare negli anni Novanta su una centrale russa, ma non voglio andare così indietro nel passato. Dobbiamo assolutamente, e quindi ben vengano questi incontri, ragionare in maniera molto precisa su quello che sta succedendo, su quello che ci aspetta e sugli strumenti che ci occorrono per arginare questo genere di attività.

Non solo, infatti, si tratta di attività in corso, ma in maniera sempre più chiara tutti gli Stati stanno mettendo nelle loro *policy* di volere e di sviluppare capacità offensive nel *cyber*-spazio. Di conseguenza, noi dobbiamo assolutamente prenderne atto.

PRESIDENTE. Ringrazio l'avvocato Mele.

Do ora la parola agli onorevoli colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Effettivamente la parte di diritto internazionale era uno degli aspetti che non avevamo trattato. Almeno per quanto mi riguarda, alcuni aspetti della Carta delle Nazioni Unite erano per me sconosciuti. Sinceramente, questo tipo d'approccio è importante.

Mi chiedo, innanzitutto, quale sia l'approccio rispetto a quello che ha la nostra Costituzione. La Francia, la Gran Bretagna hanno meno vincoli da un punto di vista costituzionale, cosa che io ritengo sia un valore per quanto mi riguarda, ma questo non vuol dire che l'applicazione di una legittima difesa e di tutte quelle parti che contemplano una legittima risposta a un attacco debbano comunque valutarsi anche nel rispetto del dettato costituzionale e, in particolare, dell'articolo 11 in entrambi i suoi commi. Questo è il primo punto.

In secondo luogo, guardando più all'adeguarsi alle prassi internazionali che ad avere chiari riferimenti di diritto, credo che già la parte militare faccia esercitazioni nel merito. Ora, non ho mai fatto un'esercitazione perché non ho mai fatto il militare, ma credo che in un'esercitazione fatta a tavolino io debba rispondere a una dichiarazione di guerra, che è ragionata *a posteriori*, cioè è qualcosa per cui valuto se ci sia un danno o meno, se ci sia un'azione che mi comporta un determinato danno.

Vorrei sapere quali limiti ha un militare nell'eventuale necessità di dover rispondere. Quell'urgenza, quel passaggio di velocità che ci ha riferito quali limiti ha da un punto di vista legale ? Quand'è che posso rispondere perché so di essere nel giusto ? Inoltre, essendo difficile la scoperta di quale sia lo Stato o l'attore dell'attacco, potrei anche sbagliare nemico perché l'IP è mascherato talmente bene che ritengo sia cinese ma, in realtà, è nordcoreano. In questo modo attaccherei stupidamente la Cina e, magari, dopo due ore scoprirei che l'IP era da un'altra parte.

Questo tipo di controreazioni, derivanti dal fatto che io debba subire un attacco che magari disabilita completamente la mia rete sanitaria, potrebbero comportare a catena una serie di danni. Nel settore fisico è molto più « semplice », o comunque ci sono gli strumenti per comprendere chi è stato.

PRESIDENTE. Vorrei integrare la domanda dell'onorevole Artini, perché su questo punto effettivamente siamo secondo me all'inizio di una riflessione e di un percorso.

Spesso non è nemmeno così semplice distinguere il confine tra difesa e offesa. L'offesa può essere presentata come il migliore, più funzionale e più efficace mezzo difensivo nel senso della prevenzione. Ce ne hanno parlato nelle missioni che abbiamo svolto relativamente all'iniziativa dell'*intelligence* nell'ambito antiterrorismo. Soffermarsi sulla definizione dei concetti

che forse devono essere ridefiniti anche dal punto di vista teorico è un problema giuridico non di poco conto.

STEFANO MELE, *Specializzato in Diritto delle tecnologie, privacy e sicurezza delle informazioni, consulente in materia di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare*. Ringrazio l'onorevole Artini e il presidente.

Parto dalla fine. C'è un problema enorme di armonizzazione dei concetti, è verissimo. Abbiamo una concezione occidentale. Peraltro, non siamo nemmeno tutti d'accordo sulla concezione occidentale di quando c'è un attacco informatico, quando ci sono dei danni, quando possiamo rispondere eccetera. La Cina, per richiamare lo Stato citato dall'onorevole Artini, ha tutto un altro approccio, anche semplicemente concettuale, a livello di strategia. Non parlano mai di *cyber-warfare*, per esempio, ma di *electronic confrontation*. È molto complesso anche solo capirsi.

Ho una minima esperienza anche a livello NATO, presso cui sono inserito anche in alcuni contesti sia formativi sia di consulenza, e c'è una difficoltà nel parlare anche tra occidentali. Effettivamente, come giustamente diceva lei, presidente, non abbiamo una definizione univoca di cosa sia un *cyber-attack*. Non ce l'abbiamo di attacco armato – nonostante la normativa risalga molto più indietro – figuriamoci se l'abbiamo di un *cyber* attacco armato, di un attacco armato in maniera più precisa fatto attraverso utilizzo delle tecnologie e della rete *Internet*.

Ho provato un po' di tempo fa a dare una definizione di cosa sia una cyber-arma; era il 2013 e quella era la prima definizione al mondo a essere data. Una parte della mia definizione è stata presa anche nel famosissimo Tallinn Manual, fatto da una parte degli esperti del NATO CCDCOE (*Cooperative Cyber Defence Centre of Excellence*) di Tallinn, ma è chiaro che sono ragionamenti slegati dal diritto internazionale.

Abbraccio, quindi, assolutamente la sua preoccupazione: in questo momento, non abbiamo definizioni, dobbiamo ragionare a livello nazionale, ma anche internazionale, sul dare le giuste parole, il giusto peso a determinate azioni. Peraltro, tornando alla domanda dall'onorevole Artini, ovviamente ripudiamo la guerra in qualsiasi sua forma, ivi compreso quindi anche questo genere di attività militare.

Vedo in questo momento la possibilità per l'Italia, anche sul piano delle tecnologie e della rete *Internet*, di seguire esattamente le stesse procedure seguite normalmente per qualsiasi attività militare. A mio avviso, non cambia niente, le tecnologie accorciano i tempi, gli spazi, cambiano qualcosa, ma se guardiamo all'essenza dei problemi, abbiamo visto anche sotto il punto di vista del diritto, che sappiamo perfettamente essere qualcosa che rincorre sempre la realtà, che a norme vecchie decine di anni si può ricorrere tuttora in un ragionamento sulle operazioni militari attraverso nuove tecnologie.

Sicuramente in questo momento dobbiamo fare anche una riflessione sotto questo punto di vista. Abbiamo necessità di comprendere come approcciarci a questo problema e, se necessario – non so se per questa specifica materia – modificare qualcosa. Ancora una volta, infatti, questa è una minaccia che ha delle percentuali di crescita che vanno a tre numeri ogni anno, cioè aumentano del cento per cento e oltre ogni anno. Noi non guardiamo che la punta della punta dell'*iceberg*. E non sto parlando di operazioni di spionaggio per loro natura segrete.

Sto parlando di operazioni che gli Stati fanno o che noi presumiamo che gli Stati facciano – dobbiamo avere le prove – nei confronti di altri Stati. In alcuni casi, però, da alcune rivelazioni divenute pubbliche si è visto che magari alcuni Stati hanno attivato le loro unità, di *intelligence* in particolare, ma anche militari – in alcuni Stati sono centralizzate – per fare attività contro società, per avvantaggiare società nazionali.

Accolgo anche la riflessione dell'onorevole Artini, che ringrazio: bisogna ragionare molto urgentemente anche dal punto di vista del diritto interno se per caso debba essere modificato qualcosa. Allo

stato attuale, non ritengo, però, che la particolarità della materia cambi poi chissà quanto lo schema che già oggi dobbiamo applicare per le operazioni militari tradizionali. Dobbiamo rispondere.

Ancora una volta, sempre rimanendo alla sua domanda, gli elementi fondamentali sono quelli che ho illustrato: per reagire dobbiamo avere la necessità di usare la forza, reagire in maniera proporzionale e nel minor tempo possibile. Ovviamente, è qualcosa che deve essere analizzata purtroppo caso per caso. In questo momento, è molto giovane la materia. Se aveste chiamato gli esperti tecnici a parlare di questa materia prima di Stuxnet, quindi prima dell'estate del 2010, la maggior parte vi avrebbe detto che gli attacchi informatici non avrebbero mai fatto il salto di qualità verso i danni fisici, che sarebbero rimasti solo danni virtuali. Il ragionamento è che un *software* che va su una macchina può, sul piano virtuale, fare tutti i danni del mondo, cancellare completamente la macchina, farle fare altro.

Una nuova tendenza su cui rifletterei molto è che ormai non parliamo più soltanto di spionaggio e di facilitazione di attacchi cinetici attraverso le tecnologie. Sempre più stiamo parlando di sottrazione di informazioni, forse anche per attività di spionaggio, modifica dell'informazione e re-immissione dell'informazione nel circuito decisionale, quindi manomissione dell'informazione, ovviamente verso il vertice societario, militare e politico.

A mio avviso, la recente uscita pubblica degli Stati Uniti d'America sulla « *cyber*-guerra » allo Stato islamico si traduce, in realtà, nel sottoporre a spionaggio elettronico le informazioni e i metodi di comunicazione dei comandanti – è pubblico – per ricalcare il metodo comunicativo, ma modificare le informazioni per cercare di stanarli, di farli uscire fuori, passare con un drone e bombardarli.

È indicativo che gli Stati Uniti d'America siano usciti pubblicamente anche con questa dichiarazione che sembra una sottigliezza, ma in realtà è l'apertura a mio avviso di un nuovo *trend* per quanto riguarda il *cyber*-spazio. Le metodologie di intossicazione informativa, infatti, risalgono all'alba dei tempi. In ogni caso, nel *cyber*-spazio è qualcosa che giudico abbastanza nuova, almeno alla luce delle mie conoscenze attuali.

Credo che anche sotto questo punto di vista dovremmo stare molto molto attenti, perché è un'operazione di spionaggio che non solo ha l'idea di sottrarre le informazioni, ma anche di rimetterle nel circuito falsificate per falsare poi l'*output* del soggetto bersaglio. Non so se ho risposto a tutta le domande.

MASSIMO ARTINI. Veramente, lo spunto riguardava solo la necessità di comprendere chi mi attacca per poi rispondere.

Ho, però, un'altra domanda. Quanto stiamo dicendo può comportare che la catena di comando non sia in condizione di prendere la responsabilità di una decisione e che, in caso d'attacco non ho un comando che decide ?

STEFANO MELE, *Specializzato in Diritto delle tecnologie, privacy e sicurezza delle informazioni, consulente in materia di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare*. Sono assolutamente d'accordo. Lo hanno creato, e quelli che non lo hanno ancora fatto stanno creando un comando specializzato per questo genere di operazioni.

Allo stesso modo, è assolutamente urgente, come si è detto anche ultimamente, che tutti i nostri militari aumentino ancora più le loro competenze in questo settore, quindi si facciano formazione ed esercitazioni mirate. In realtà, le stanno già facendo. Personalmente, insegno questo genere di materie da almeno tre o quattro anni alla Scuola di guerra aerea a Firenze, all'ISMI, quindi non credo che sia *tabula rasa*.

Fortunatamente, anzi soprattutto le nostre Forze armate sono già da tempo attente a queste problematiche. Dobbiamo fare, però, decisamente molto di più, dobbiamo anche strutturarci sia a livello governativo, come giustamente diceva lei – e io sposo la sua idea – sia a livello organizzativo per creare un comando. Dico

*cyber-command* e automaticamente viene in mente quello che è stato creato dagli Stati Uniti d'America ormai qualche anno fa. In realtà, però, avete visto che ho fatto l'introduzione appositamente focalizzandomi su quello che stanno facendo gli altri Stati.

Al di là degli Stati Uniti d'America, che sono tanti anni avanti, la Cina sta facendo questo, centralizzando e mettendo insieme *intelligence* e Forze armate sotto un unico comando, addirittura nello stesso posto, per fare solo *cyber*. Il Regno Unito, la Danimarca, l'Australia, la Russia, Israele e tutti i Paesi che volete, stanno facendo la stessa cosa. Anche a livello europeo, stanno facendo tutti così, quindi bisogna necessariamente agire in questo senso, creare un comando militare operativo specifico e specializzato per questo genere di operazioni militari con strumenti per fare attività di investigazione e, contemporaneamente, per capire che non si può sbagliare nel rintraccio, e quindi nell'IP, per tornare all'esempio, che sembra cinese ma è nordcoreano.

Non si può e non si deve sbagliare, perché questo comporta, dal punto di vista del diritto interno, e va bene, ma soprattutto del diritto internazionale una problematica enorme. A sua volta, infatti, lo Stato che si vede attaccato e sa che non ha fatto niente potrebbe prendere quello come un attacco, come un uso della forza o, addirittura, un attacco armato, perché magari abbiamo risposto cineticamente a un attacco informatico perché possiamo farlo.

È fondamentale, allora, creare un nucleo militare che faccia solo questo e abbia dentro persone di alto profilo, che sappiano fare i comandanti militari, ma anche dei tecnici che facciano operazioni e difesa. La risposta all'*active server defence* di cui diceva il presidente è assolutamente sì. Cerchiamo di farlo. Il C4 Difesa cerca di farla e lo fa molto bene a difesa dei nostri interessi nazionali dal punto di vista militare.

Bisogna, però, cercare di sviluppare e concentrare a mio avviso le forze, formarle e ricordarci che nel *cyber*-spazio non esistono poligoni di tiro in questo momento per diventare bravi in questo genere di attività. Non è come per le nostre Forze armate, che hanno i poligoni di tiro e a cui si insegna a utilizzare un'arma. Nel *cyber*-spazio bisogna fare per impratichirsi di questo genere di attività. Moltissime operazioni « militari » o di *intelligence* che risalgono ad anni precedenti e che potevano essere attribuite ad alcuni Stati, che si mascheravano magari dietro il nome di Anonymous, quindi cercavano di distrarre un po', a mio avviso molte volte erano fatte per imparare, verificare e testare le capacità o nuovi strumenti informatici, che poi hanno creato il cosiddetto *cyber*-armamento, che apre tutto un altro scenario.

ANGELO TOFALO. Ne approfitto per una domanda data la sua deformazione professionale e la grande competenza in ambito normativo giuridico sulla *cyber*. Lei ci ha delineato un ottimo quadro della situazione attuale e anche della direzione futura. Da ignorante in materia penso all'ultimo anno, al caso di spionaggio industriale Volkswagen, o al caso certo di Hacking Team, dove c'è stata infiltrazione di dati.

Vorrei ragionare sugli ultimi anni in termini di sistema Paese, quindi al di là dello stato dei ministeri che subiscono continuamente attacchi cibernetici, delle aziende strategiche, come ENI, ENEL, ENAV, che comunque ogni giorno subiscono attacchi, estendo anche alla piccola e media impresa, di cui oggi finalmente si parla molto. Anche il piccolo imprenditore, infatti, magari non addentro alla materia, quando perde il terzo, il quarto, il quinto cliente, inizia a chiedersi che cosa stia succedendo.

Negli ultimi anni, stanno aumentando queste denunce, queste controversie ? Che tempi si hanno ? Ho citato Hacking Team come caso eclatante per l'opinione pubblica di livello mondiale, ma ragionando solo per l'Italia, restando solo nel nostro Paese – se avesse anche altri dati, sarebbe utile conoscerli – che tempi ci sono per arrivare alla fine, alle sentenze ?

STEFANO MELE, *Specializzato in Diritto delle tecnologie, privacy e sicurezza*

*delle informazioni, consulente in materia di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare*. La ringrazio, onorevole Tofalo, per la domanda molto interessante.

Effettivamente, c'è un incremento enorme dell'attività, ma c'è anche – a mio avviso – un decremento delle denunce da parte delle aziende, soprattutto private. Le spiego facilmente il perché: per il danno all'immagine. Faccio l'avvocato, sono all'interno di alcune aziende, e si verificano delle cose. Ci sono protocolli firmati con DIS, il CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche), il CERT (*Computer Emergency Response Team*) della dottoressa Forsi.

Ogni volta che salta fuori un incidente informatico, e ne saltano fuori, ci si riunisce, si dice che siamo obbligati – in Italia, come sa perfettamente, senza una norma non si fa nulla, scusate la franchezza, ma da avvocato purtroppo rilevo questo – e tendiamo a dare il meno possibile: se viene fuori, è un danno all'immagine incalcolabile, va sui giornali, quindi su *Internet*, e allora non si cancella più.

Questa è una visione a mio avviso molto miope della problematica. Posso comprenderla da un punto di vista professionale, quindi da avvocato, non la comprendo come appassionato di queste materie. Nel lungo periodo questo ci porta alla situazione attuale in cui abbiamo contezza nemmeno del 10 per cento di quello che avviene realmente. Ancora una volta, non parlo di attività di spionaggio.

Lei ha giustamente chiamato in causa le piccole e medie imprese, che ricordo a me stesso sono il 99,9 per cento della presenza delle società sul nostro territorio e il 99,8 per cento a livello europeo, producono poco più del 60 per cento della nostra ricchezza e, quindi, sono il terreno su cui dovremmo andare prima di tutto, prima ancora che sulle grandi. Queste aziende non hanno i soldi per permettersi un *software*, due ingegneri informatici che gestiscono i sistemi, e quindi non lo fanno. Mi dicono e dicono che devono investire quei soldi – l'investimento non è nemmeno piccolissimo – in altro.

Se sono uno Stato che vuole sottrarre, attraverso attività di spionaggio elettronico e informatico, i nuovi progetti della Ferrari, perché devo andare a cercare di violare i sistemi informatici della Ferrari, dove ci sono moltissimi ingegneri informatici e un *budget* elevato per proteggere quegli *asset*, quando posso andare tranquillamente dal brianzolo che produce i bulloni della Ferrari e ha il disegno della Ferrari a portata di mano ? Lo faccio fare anche all'ultimo ragazzino che ho incrociato per strada e ho ottenuto lo stesso risultato.

Questa è la pericolosità per il sistema Paese. Ed è questo che mi spinge a riflettere e a dire, anche spesso pubblicamente, e quindi lo ribadisco anche in questo caso, che lo spionaggio elettronico costituisce da sempre, in particolare dagli ultimi dieci anni, la vera minaccia per la sicurezza economica, e quindi anche la sicurezza nazionale, di qualsiasi Paese al mondo. È attraverso queste logiche che gli Stati o le altre società – lo spionaggio industriale è un'altra problematica, ma sotto il punto di vista del diritto penale interno dello Stato che subisce – si muovono.

Oltretutto, per tornare alle norme, se sotto questo punto di vista ne abbiamo, sotto quello dell'*intelligence* non ce ne sono. Abbiamo soltanto un protocollo addizionale – vado a memoria – degli anni Quaranta che parla addirittura di spie travestite beccate sul territorio dello Stato all'interno del quale stavano svolgendo attività. Anche in quel caso, però, qualora la spia venga presa non ne risponde lo Stato per cui la spia lavora, ma la spia personalmente. Non ci sono tutte le garanzie.

Dal punto di vista del diritto internazionale non ci sono, cioè, norme sullo spionaggio in generale, figuriamoci lo spionaggio elettronico, semplicemente perché tutti gli Stati spiano, tutti gli Stati hanno sempre spiato e tutti gli Stati vogliono continuare a spiare. Questa è una problematica. Ovviamente, c'è anche uno spionaggio militare. Siamo assolutamente d'accordo, quindi, sulle piccole e medie imprese.

PRESIDENTE. Ringraziamo molto l'avvocato Mele per le informazioni e le osservazioni proposte. Lo ringrazio anche per la documentazione che ci ha lasciato, di cui autorizzo la pubblicazione in allegato al resoconto stenografico dell'audizione *(vedi allegato)*. Se dovessimo avere bisogno ancora di lei, la contatteremo.

Dichiaro conclusa l'audizione.

**La seduta termina alle 16.50.**

*IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE*

DOTT. RENZO DICKMANN

*Licenziato per la stampa il 13 giugno 2016*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

# LA REAZIONE LEGITTIMA DI UNO STATO AD UN ATTACCO INFORMATICO

Stefano Mele

COMMISSIONE DIFESA - CAMERA DEI DEPUTATI

28 APR. 2016

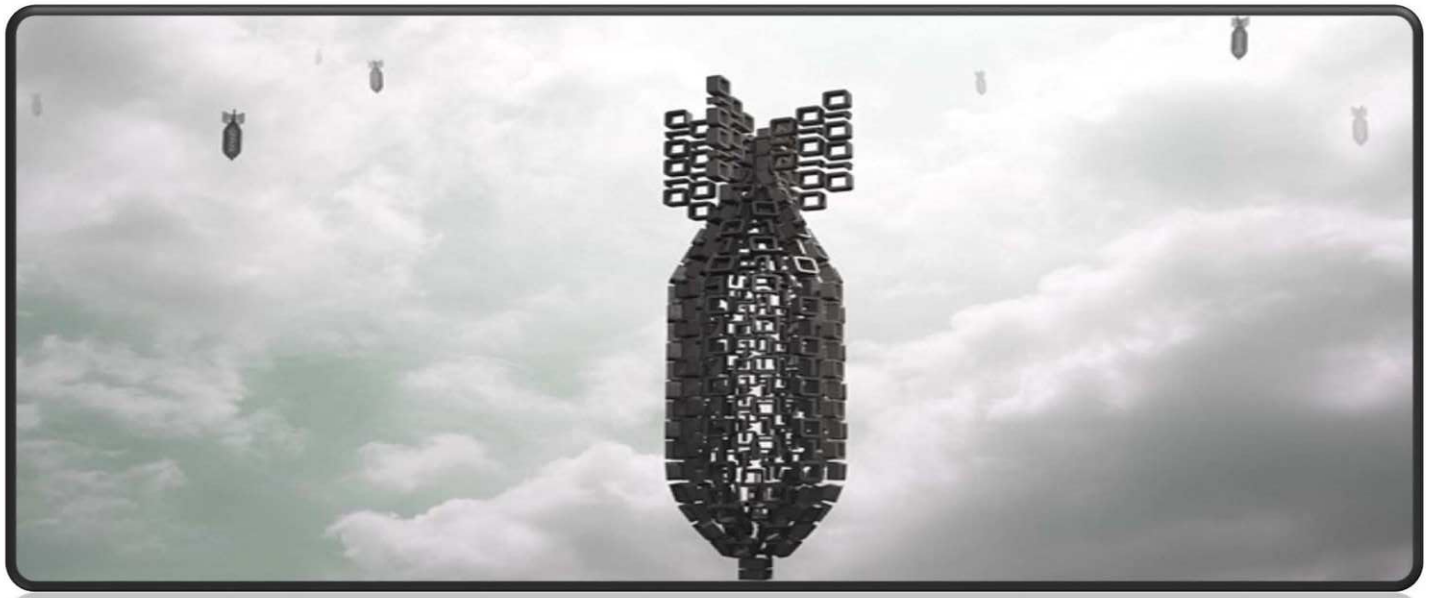
ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# @MeleStefano

- Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza ed Intelligence presso Carnelutti Studio Legale Associato di Milano
- Socio fondatore e Partner del Moire Consulting Group
- Dottore di ricerca presso l'Università degli Studi di Foggia e collaboratore presso le cattedre di Informatica Giuridica e Informatica Giuridica avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano
- Presidente del «*Gruppo di Lavoro sulla Cyber-security*» della Camera di Commercio Americana in Italia (AMCHAM)
- Esperto di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare:
  - Coordinatore dell'Osservatorio "*InfoWarfare e Tecnologie emergenti*" dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli'
  - Docente presso numerosi Istituti di formazione e di ricerca del Ministero della Difesa italiano e in ambito NATO
- La NATO lo ha inserito nella lista dei suoi *Key Opinion Leaders for Cyberspace Security*
- La rivista *Forbes* lo ha inserito tra i 20 migliori *Cyber Policy Experts* al mondo da seguire in Rete

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Stati ed attività di cyber-warfare



*La reazione legittima di uno Stato ad un attacco informatico*

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Stati ed attività di cyber-warfare

- In via preliminare, occorre evidenziare come, al di là del clamore mediatico che fantomatiche "cyber-war" hanno da tempo guadagnato nell'immaginario dell'opinione pubblica, l'utilizzo del cyber-spazio e delle tecnologie per scopi militari ha finora assunto - nella pratica - il solo **ruolo di facilitatore di attacchi cinetici attraverso i quattro domini tradizionali** (aria, terra, mare e spazio)

- L'approccio strategico sta cambiando molto velocemente: da una mera difesa attiva (*Active Cyber-Defence*) ad un vero e proprio **sviluppo di capacità offensive** per il cyber-spazio

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Stati ed attività di cyber-warfare

## STATI UNITI

- L'aspetto più rilevante della dottrina sulle "*Cyberspace Operations*" è certamente legato al formale riconoscimento e impiego da parte degli U.S. delle attività militari offensive volte a "*proiettare la forza nel e attraverso il cyber-spazio*", al fine di "*degradare, danneggiare o distruggere l'accesso, il funzionamento o la disponibilità delle capacità di un bersaglio ad un livello e per un periodo di tempo determinato*"
- *Offensive Cyber Operations* volte a "*controllare o modificare le informazioni, i sistemi informatici o le reti dell'avversario*"
- Attività, queste, tutte intimamente legate ad uno specifico ordine esecutivo di autorizzazione e aventi come unico possibile bersaglio diretto dell'attacco un "*obiettivo militare*"

*La reazione legittima di uno Stato ad un attacco informatico*

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Stati ed attività di cyber-warfare

## CINA

- Il 31 dicembre 2015, la Central Military Commission cinese ha pubblicamente annunciato di aver completato una sostanziale riforma organizzativa della People's Liberation Army, ovvero le Forze Armate cinesi, dando alla luce tre nuovi organismi: l'Army Leading Organ, la Rocket Force e la Strategic Support Force
- Tra le tre, la Strategic Support Force appare essere la più interessante sotto il punto di vista della cyber-security
- Secondo alcune fonti, sarebbe a sua volta costituita da tre ramificazioni: la prima, responsabile delle operazioni militari e di intelligence - sia difensive, che offensive - nel e attraverso il cyber-spazio; la seconda, deputata alle operazioni militari condotte nello spazio, in cui rientrerebbero anche le attività di sorveglianza e quelle inerenti ai satelliti; la terza, infine, con compiti di Electronic Warfare (EW), sia dal punto di vista offensivo, che difensivo e di intelligence (ELINT)

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

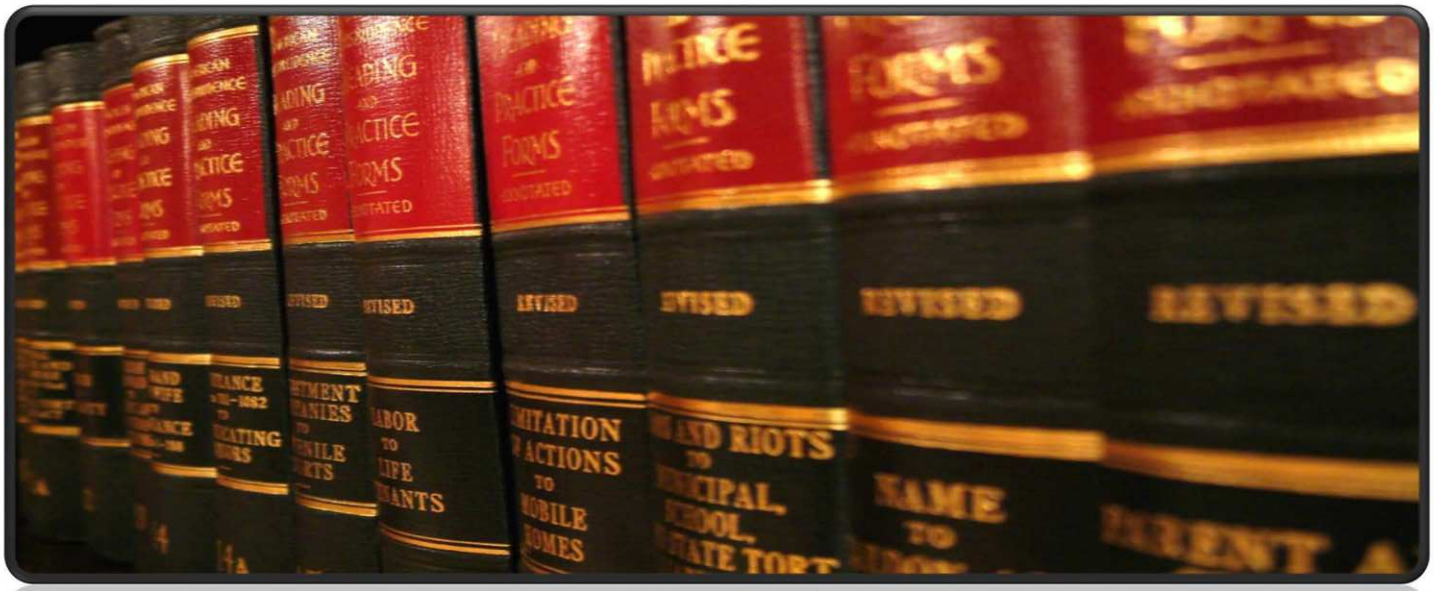
# #Stati ed attività di cyber-warfare

## REGNO UNITO

- Il 23 novembre 2015, il Regno Unito ha pubblicato il suo nuovo "Strategic Defense and Security Review", uno dei documenti più rilevanti per comprendere la postura strategica del governo inglese in ambito di difesa e sicurezza nazionale per i prossimi cinque anni
- Il governo inglese ha previsto, tra le altre cose, che le proprie Forze Armate conseguano capacità militari offensive avanzate nel e attraverso il cyber-spazio, così come previsto dal "*National Offensive Cyber Programme*" gestito in partnership dal Ministero della Difesa inglese e dal Government Communications Headquarters (GCHQ)

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato



ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

**La mancanza di norme specifiche sul piano del diritto internazionale non esclude che possano identificarsi delle norme consuetudinarie potenzialmente applicabili**

**Questa estensione è consentita ad esempio dalla clausola Martens, comparsa per la prima volta nel preambolo della IV Convenzione dell'Aia e ripresa nelle quattro Convenzioni di Ginevra del 1949, che ha una portata generale ed è volta a colmare eventuali lacune nella codificazione del diritto internazionale**

ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

**Peraltro, riconoscendo la crescente importanza del dominio cibernetico, già nel 2013, durante la riunione del *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* delle Nazioni Unite, si è convenuto che il diritto internazionale vigente si applica anche all'interno del dominio cibernetico, così come i concetti tradizionali di sovranità statale**

ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

**Nel 2015, invece, sempre il *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* delle Nazioni Unite, ha convenuto che:**

a. **Gli Stati esercitano la loro giurisdizione sulle infrastrutture informatiche situate sul loro territorio**
b. **Nell'utilizzo degli strumenti informatici, gli Stati, devono rispettare, oltre agli altri principi di diritto internazionale, quello dell'inviolabilità della sovranità territoriale altrui, della parità tra le diverse sovranità territoriali, il principio dell'assestamento dei conflitti mediante mezzi pacifici e la non ingerenza nelle questioni interne di altri Stati. I vincoli legali internazionali già esistenti sono applicabili anche all'utilizzo da parte degli Stati di strumenti informatici. Gli Stati devono comunque adempiere alle obbligazioni loro derivanti dagli accordi internazionali riguardo la protezione dei diritti umani e le libertà fondamentali**
c. **[…]**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

**Nel 2015, invece, sempre il *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* delle Nazioni Unite, ha convenuto che:**

d. **Il Gruppo ha osservato il consolidarsi di questi principi internazionali, incluso, dove possibile, quelli di umanità, necessità, proporzionalità e distinzione;**
e. **Gli Stati non possono commettere atti internazionalmente illeciti mediante strumenti informatici neanche attraverso deleghe a parti terze che operino su indicazione dello Stato in questione e devono assicurarsi del fatto che il loro territorio non sia utilizzato da attori non statali al fine di commettere tali atti**
f. **Gli Stati devono adempiere i loro doveri riguardo agli atti internazionalmente illeciti a loro riconducibili secondo il diritto internazionale. Comunque sia, indizi sul fatto che un attacco informatico sia stato lanciato o abbia origine dal territorio di uno Stato o da un'infrastruttura informatica appartenente a questo, non sono sufficienti ad attribuire suddetta attività allo Stato in questione. Il Gruppo ha osservato che l'accusa di organizzare o supportare atti illeciti contro un altro Stato deve essere comprovata**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

**Possono evidenziarsi, pertanto, alcuni elementi interessanti nella prassi degli Stati in ordine all'applicazione delle norme riguardanti lo *ius ad bellum* contenute nella Carta delle Nazioni Unite alle operazioni informatiche**

ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite

**Art. 2(4): «Tutti gli Stati membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite»**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

Questo articolo è stato ritenuto applicabile ed essenziale alle operazioni informatiche per garantire un ambiente digitale aperto, sicuro, pacifico ed accessibile

Perché l'estensione a questo contesto sia possibile sono necessarie tre condizioni: (1) che la condotta sia imputabile ad uno Stato, in quanto la norma non è riferita a individui privati o gruppi armati; (2) che l'azione possa essere classificata come una minaccia o un utilizzo della forza; (3) che ciò avvenga nell'ambito delle relazioni internazionali

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(1) che la condotta sia imputabile ad uno Stato**

**La International Law Commission ha stilato un progetto di articoli sulla responsabilità degli Stati, successivamente approvato dall'Assemblea Generale, in cui introduce una serie di criteri grazie ai quali è possibile attribuire una condotta ad uno Stato, molti dei quali sono applicabili anche in ambito informatico**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(1) che la condotta sia imputabile ad uno Stato**

**L'articolo 4 che stabilisce che «il comportamento di un organo statale sarà considerato come un atto dello Stato ai sensi del diritto internazionale, sia che tale organo eserciti funzioni legislative, esecutive, giudiziarie o altre, qualsiasi posizione abbia nell'organizzazione dello Stato e quale che sia la sua natura come organo del governo centrale o di un'unità territoriale dello Stato»**

**L'articolo prosegue definendo l'organo come «qualsiasi persona o ente che rivesta tale posizione secondo il diritto interno dello Stato»**

ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(1) che la condotta sia imputabile ad uno Stato**

**L'articolo 5 disciplina anche quei casi in cui l'azione non sia perpetrata da un organo dello Stato, bensì da un soggetto che venga in qualche modo abilitato dal diritto di quello Stato ad esercitare prerogative di governo**

**Potrebbe essere il caso in cui l'attaccante sia membro di un ente parastatale, pubblico, semi-pubblico o di una società privatizzata autorizzata ad esercitare un qualche tipo di prerogativa governativa**

ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(1) che la condotta sia imputabile ad uno Stato**

**L'articolo 11 ritiene che comunque una condotta non attribuita ad uno Stato ai sensi degli articoli precedenti può comunque essere sua responsabilità qualora questi ne sia a conoscenza e la adotti come propria**

**L'ultimo caso qui preso in considerazione è quello in cui le operazioni provengono da strutture informatiche presenti sul territorio che non vedono alcun coinvolgimento dello Stato. In questo caso quest'ultimo potrebbe essere accusato di non aver adottato le necessarie misure preventive**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(2) che l'azione possa essere classificata come un utilizzo della forza**

**Riguardo al secondo requisito, nonostante non esista una definizione univoca di 'uso della forza', un'azione informatica potrebbe essere classificata come tale nel momento in cui la sua intensità e i suoi effetti siano paragonabili a quelli di un attacco armato**

**In questo caso è preferibile utilizzare come criterio di classificazione quello della gravità degli effetti che conseguono dall'attacco**

**Attività di spionaggio, di sabotaggio o attività criminali non costituirebbero un uso della forza, lo sarebbero con certezza quegli atti che abbiano come effetto quello di danneggiare infrastrutture fondamentali**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 2(4)

**(3) che ciò avvenga nell'ambito delle relazioni internazionali**

**Con la terza condizione si vuole sottolineare che non solo la minaccia deve provenire da uno Stato, ma implicitamente deve anche essere rivolta ad un membro della comunità internazionale**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite

**Art. 51: «Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale»**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 51

**La legittima difesa può essere definita come la possibilità per uno Stato di rispondere, se necessario, ad un illegale uso della forza che corrisponda ad un attacco armato**

**La legittima difesa è considerata sia un diritto innato dello Stato che un'eccezione al divieto dell'uso della forza e l'inclusione di questo nella Carta delle Nazioni Unite ha una duplice valenza: da una parte vuole riconoscere il preesistente diritto degli Stati, dall'altra vuole porre le basi alla possibilità di una legittima difesa collettiva**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 51

**La Corte Internazionale di Giustizia ha stabilito che l'art. 51 si applica a qualsiasi uso della forza, indipendentemente dal mezzo utilizzato, di conseguenza emerge qui la possibilità di estenderlo anche all'ambito informatico**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 51

Anche se non esiste una definizione universale, con "attacco armato" si intende: "an armed attack is considered to be a use of force originating outside the target State's territory that rises above the level of a small-scale, isolated armed incident or criminal activity, and which is directed against a State's territory, its military vessels or aircraft in international waters or airspace or lawfully present in another State's territory, or, in certain situations, directed against its nationals located abroad"

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 51

**Riferito allo strumento informatico un attacco armato potrebbe consistere in un'operazione informatica diretta contro le infrastrutture fondamentali dello Stato qualora avesse le potenzialità di compromettere seriamente le sua capacità di svolgere le proprie funzioni o possa minare la sua stabilità politica, economica e sociale per un lasso di tempo prolungato, e ciò potrebbe avvenire anche in assenza di evidenti danni fisici**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Reazione legittima di uno Stato

## Carta delle Nazioni Unite - art. 51

**Le condizioni perché si possa invocare la legittima difesa sono:**

**Attacco armato: di cui abbiamo già parlato**

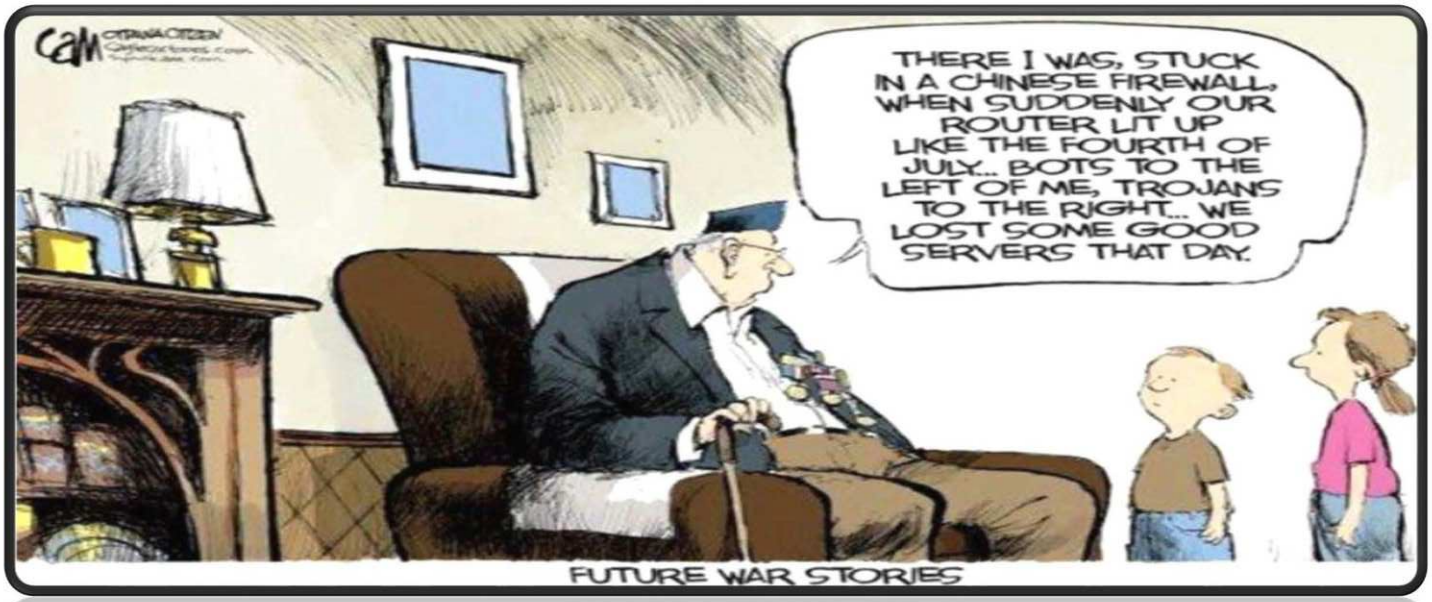
**Necessità: la necessità dell'uso della forza presuppone un pericolo imminente e la mancanza di altre possibili soluzioni pacifiche**

**Proporzionalità: si riferisce alla necessità che le contromisure adottate in virtù del diritto di legittima difesa non eccedano la misura necessaria per reprimere o respingere l'attacco**

**Immediatezza: richiede che lo Stato reagisca nel minor tempo possibile o comunque in un lasso di tempo ragionevole**

ISTITUTO ITALIANO di STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli

# #Conclusioni



ISTITUTO ITALIANO DI STUDI STRATEGICI
ITALIAN INSTITUTE OF STRATEGIC STUDIES
Niccolò Machiavelli
DOMANDE..?
28 APR. 2016
@MeleStefano
s.mele@strategicstudies.it

*17STC0017460*