OPINIO JURIS
LAW & POLITICS REVIEW

LA DISCIPLINA GIURIDICA DEL *CYBERSPACE*

UNA PANORAMICA SULLE PROBLEMATICHE ATTUALI E LE PRINCIPALI LINEE EVOLUTIVE

di

Matteo Mirti

SOMMARIO: I. Aspetti problematici del cyberspace e strategie operative degli Stati - II. La prospettiva delle Nazioni Unite - III. La prospettiva delle organizzazioni regionali – IV. Direttrici dello sviluppo normativo – V. Principali questioni emerse in dottrina – VI. Il problema della Sovranità nel cyberspace.

Le tecnologie informatiche costituiscono attualmente un nuovo dominio della conflittualità all'interno del quale, gli attori che vi interagiscono, statali e non, sviluppano relazioni suscettibili tanto di contribuire allo sviluppo dell'umanità, quanto, al contempo, di costituire una minaccia alla pace e alla sicurezza internazionali. Le caratteristiche tecniche del *cyberspace* incidono sui comportamenti e sulle modalità di azione che i diversi attori possono porre in essere utilizzando le tecnologie informatiche. Ciò ha spinto, negli ultimi anni, sia gli Stati che le organizzazioni internazionali più importanti, a definire delle strategie politiche, volte a migliorare la sicurezza del ciberspazio e l'efficacia della loro azione in questo dominio.

Dal punto di vista giuridico si pone il problema di delineare una disciplina del *cyberspace* che tenga conto della necessità sia di implementarne lo sviluppo, sia di disciplinare i comportamenti degli attori che operano in questo contesto. Intento del presente contributo è quello di fornire una panoramica generale dello stato della discussione giuridica sul punto.

I. *Aspetti problematici del cyberspace e strategie operative degli Stati e delle organizzazioni internazionali* - L'attacco *cyber* subito dall'Estonia nel 2007[1] ha messo in luce la vulnerabilità dello Stato di fronte alle nuove tecnologie. La vicenda rappresenta, assieme all'attacco ai sistemi informatici di gestione delle centrali nucleari iraniane[2], l'esempio più completo delle potenzialità offensive delle tecnologie informatiche. In

[1] cfr. CHRISTIAN CZOSSECK, RAIN OTTIS, ANNA-MARIA TALIHÄRM, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational*, International Journal of Cyber Warfare and Terrorism, 24-34, January-March 2011.

[2] cfr. U. GORI, S. LISI, *Information Warfare 2012, Armi cibernetiche e processo decisionale,* Franco Angeli, Milana, 2013.

quell'occasione, infatti, l'Estonia ha visto compromessa la funzionalità dei suoi servizi essenziali, dalla fornitura di acqua potabile alle transazioni bancarie.

Da quel momento i rischi derivanti dall'uso delle *Information and Communications Technologies* (ICTs) sono stati oggetto di discussione, tanto sul piano politico e militare, quanto sul piano del diritto e delle forme di cooperazione internazionale.

Secondo una definizione data nel 2010 da Wiliam J. Lynn III, allora Vice Segretario della Difesa americano, il *cyberspace* rappresenta «*il quinto dominio della conflittualità*»[3], dopo terra, mare, aria e spazio.

Rispetto ai tradizionali domini, tuttavia, il ciberspazio presenta caratteristiche proprie, del tutto peculiari[4].

Il *cyberspace* è un'opera dell'uomo, come tale suscettibile di continue evoluzioni, strutturali e funzionali, tali da determinarne, potenzialmente, persino la chiusura. Ciò pone di per se, ogni parte del ciberspazio od ogni attività in esso svolta in posizione di costante rischio. Da questo punto di vista si può parlare di interesse pubblico globale alla persistenza delle reti informatiche.

Al suo interno operano, soggetti difficilmente individuabili e portatori di interessi suscettibili di entrare in contrasto per ragioni non riscontrabili nelle conflittualità determinata da altri domini.

Le caratteristiche del *cyberspace* che, più di altre, sollevano problemi, sono tuttavia legate alla mancanza di confini ed alla contemporaneità tra azione ed evento. Da una parte, infatti, l'assenza di una ripartizione spaziale priva i diversi "settori" del ciberspazio della propria indipendenza, così evidenziando il problema dell'individuazione, per ogni uno di essi, di un potere "amministrativo". Dall'altra, l'ubiquità informatica, ossia la contemporaneità tra azione ed evento, che si concretizza nello spazio reale in punti distanti, rende difficile la reazione.

L'emergere di un nuovo, particolare, spazio entro cui interagire, ha posto al centro delle agende politiche dei principali Stati il problema di individuare strategie e forme di tutela degli interessi nazionali coinvolti[5]. Allo stato attuale documenti strategici in materia sono stati resi pubblici da 79 Stati, a cui devono aggiungersi quelli predisposti dall'Unione Europea, dall'Organizzazione del Trattato dell'Atlantico del Nord, dall'Organizzazione per la Cooperazione e lo Sviluppo Economico e dall'Associazione delle Nazioni del Sud-Est Asiatico (in prosieguo, rispettivamente, UE, NATO, OCSE e ASEAN).

[3] cfr. WILLIAM J. LYNN III, *Defending e new domain: the Pentagon's cyber strategy*, Foreign Affairs 2010, p. 97.

[4] cfr. IACOPO CHIARUGI, NICCOLÒ DE SCALZI, LUIGI MARTINO, MARCO MAYER, *La politica internazionale nell'era digitale. Dispersione o concentrazione del potere?*, in *Intelligence e interesse nazionale*, a cura di UMBERTO GORI, LUIGI MARTINO, Aracne Editrice, 2015; RAFFAELE AZZARONE, *Cyber Vademecum*, GNOSIS Rivista Italiana di Intelligence, 2014; GIANLUCA ANSALONE, *Cyberspazio e nuove sfide*, GNOSIS 3/12.

[5] cfr. ALESSANDRO FASANI, *Analisi della necessita di una migliore cyber security per le infrastrutture critiche,* in *Intelligence e interesse nazionale*, a cura di UMBERTO GORI, LUIGI MARTINO, Aracne Editrice, 2015.

L'analisi di tali documenti[6], non ultimo quello italiano[7], permette di evidenziare come gli Stati individuino alcuni pilastri strategici comuni. In particolare, emerge il ruolo centrale attribuito all'identificazione ed alla classificazione delle infrastrutture critiche da proteggere, nonché alla predisposizione di trattati, leggi e regole di condotta nazionali ed internazionali. In altri termini, il problema che si pone è quello di individuare il bene oggetto di tutela e le forme ed i limiti giuridici dei comportamenti adottabili dagli operatori del ciberspazio.

II. *La prospettiva delle Nazioni Unite* – Le problematiche dettate dal *cyberspace* sono state – e tuttora sono - oggetto di analisi giuridica, oltre che dalla comunità scientifica, anche a livello internazionale, nel contesto di organizzazioni sia di carattere universale sia di carattere regionale.

Nel gennaio del 2016, l'Assemblea Generale delle Nazioni Unite, ha formalmente adottato una risoluzione sulla sicurezza informatica[8], il cui testo, precedentemente approvato dal Primo Comitato dell'Assemblea Generale, specializzato in sicurezza internazionale e disarmo, fa proprio il rapporto presentato dal *Group of Governamental Expert* (di seguito GGE)[9] istituito dal Segretario Generale nel 2014 con sua risoluzione n. 68/243.

In tale risoluzione, l'Assemblea Generale afferma che gli sviluppi nel settore ICTs «*semble offrir de très vastes perspectives pour le progrès de la civilisation, la multiplication des possibilités de coopération pour le bien commun de tous les Etats le renforcement du potentiel créatif de l'humanité et l'amelioration de la circulation de l'information dans la communauté mondiale*» e nota, inoltre, «*que la diffusion et l'emploi des technologies et moyens informatiques intéressent la communauté internazionale tout entière et qu'une vaste coopération internazionale contribuira à une efficacité optimale*».

Lo spazio *cyber* viene in tal modo riconosciuto, quanto meno sul piano politico, quale interesse proprio della Comunità Internazionale, in ragione dalle potenzialità offerte dalle nuove tecnologie al progresso dell'umanità.

Tuttavia, affianco agli aspetti positivi, l'atto dell'Assemblea Generale evidenzia come questa stessa tecnologia «*risquent d'etre utilises à des fin incompatibles avec le maintien de la*

[6] cfr. STEFANO MELE, *I principi strategici delle politiche di cyber security*, Sistema di informazione per la sicurezza della Repubblica, http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html.

[7] cfr. PRESIDENZA DEL CONSIGLIO DEI MINISTRI, Quadro strategico per la sicurezza dello spazio cibernetico, Dicembre 2013; a cura di ROBERTO BALDONI, ROCCO DE NICOLA, *Il futuro della Cyber Security in Italia,* Laboratorio Nazionale di Cyber security, Consorzio Interuniversitario Nazionale per l'Informatica, DIS, ottobre 2015.

[8] cfr. Assemblea Generale delle Nazioni Unite, risoluzione n.70/237; HENDERSON, *The United Nations and the Regulation of Cyber-security*, in N. TSAGOURIAS, R. BUCHAN (eds), *Research Handbook on International Law and Cyberspace* , Edward Elgar, 2015.

[9] cfr. Assemblea Generale delle Nazioni Unite, documento A 70/174.

stabilité et de la sécurité internationales et de porter atteinte à l'integrité de l'infrastructure des Etats, nuisant ainsi à leur sécurité dans les domaines tant civil que militaire».

Rispetto ai rischi evidenziati nella risoluzione, il Segretario Generale aveva, come accennato, costituito precedentemente il GGE, attribuendo ad esso lo specifico mandato[10] di procedere, da un lato, alla disamina delle possibili minacce alla sicurezza informatica e delle misure adottabili dagli Stati per farvi fronte, e, dall'altro, di valutare i possibili conflitti nel dominio *cyber* e l'applicabilità, in questo ambito, del diritto internazionale.

III. *La prospettiva delle organizzazioni regionali* - Le problematiche relative allo spazio *cyber* sono state affrontate anche a livello regionale, dall'UE, dalla NATO, dall'OCSE e dall'ASEAN *Regional Forum*.

Nel contesto europeo la protezione dello spazio *cyber* viene presa in considerazione da due diversi punti di vista. Da una parte essa viene legata alla crescita economica e allo sviluppo di un uso consapevole e responsabile dei mezzi informatici da parte degli utenti; da un'altra, essa rileva sotto il profilo del contrasto al crimine informatico e della messa in sicurezza delle infrastrutture critiche nazionali informatizzate.

Il concetto di *cyber security* viene definito a livello europeo come l'insieme di precauzioni ed interventi che si possono prendere per proteggere il *cyber* dominio, in campo sia civile che militare, dalle minacce associate o che possono nuocere alle reti ed alle infrastrutture di informazione interdipendenti.

In tal senso si esprime la «Strategia dell'Unione europea per la sicurezza» del Febbraio 2013. Questa fa seguito ad una serie di documenti in cui l'Unione europea aveva delineato un suo originale percorso nell'approccio alla difesa del *cyberspace* di cui, la strategia, può dirsi ne faccia una sintesi[11].

Suo scopo principale è quello di garantire uno spazio *cyber* «aperto e sicuro», in cui trovino affermazione *a)* i principi di protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della *privacy*; *b)* il principio dell'accesso alla rete garantito per tutti; *c)* la realizzazione di forme di *governance* che coinvolgano i diversi *stakeholder* in maniera democratica ed efficiente; *d)* il principio della responsabilità condivisa tra tutti gli attori coinvolti.

Tali principi hanno la funzione di *α) raggiungere la sicurezza informatica; β)* ridurre drasticamente il *cyber crime*; *γ)* sviluppare una politica e una capacità di *cyber* difesa

[10] cfr. Segretario Generale delle Nazioni Unite, risoluzione n. 68/243; ELAINE KORZAK, *Cybersecurity at the UN: Another Year, Another GGE*, https://www.lawfareblog.com/cybersecurity-un-another-year-another-gge.

[11] cfr. CLAUDIA CONCETTI, *Cybersecurity: Unione Europea e Italia Prospettive a Confronto*, Quaderni IAI, Edizioni Nuova Cultura, 2014; EMANUELA C. DEL RE, *Sicurezza europea le nuove sfide*, GNOSIS, 1/2013; NICOLA PEDDE, *Cybersecurity Strategy of The European Union*, GNOSI, 4/2012; FRANCESCO BUTTINI, *Cyber security: modelli a confronto*, in *Intelligence e interesse nazionale*, a cura di UMBERTO GORI, LUIGI MARTINO, Aracne Editrice, 2015.

connesse alla Politica Europea di Sicurezza e di Difesa (PESD); *δ)* creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costituiti di quest'ultima.

L'approccio dell'Unione europea si caratterizza, da altro punto di vista, per l'aver sviluppato una dimensione "istituzionale" della *cyber security* individuando vari uffici ed organi, competenti per i vari aspetti, a livello comunitario e nazionale.

Affianco all'Unione europea può essere presa in considerazione l'OSCE, la cui azione rispetto al *cyberspace* può essere descritta prendendo a riferimento il *workshop* tenuto a Belgrado, il 30 ottobre del 2015 e la Decisione n. 1202 del 10 marzo 2016.

A Belgrado l'attenzione veniva posta sull'individuazione e l'adozione di strategie prettamente *cyber* da un lato e, dall'altro, sull'adozione di meccanismi di cooperazione che, sviluppando il principio di trasparenza riducono il rischio di un conflitto tra Stati. In questa direzione muove in particolare la Decisione n. 1202 la quale individua *Confidence-Building Measures* (CBMs).

L'idea che, nell'azione dell'OCSE, sorregge tali norme è quella, mutuata dall'era della Guerra Fredda, di avere un sistema di comunicazione diretta tra Stati che eviti il conflitto e prevenga *escalation* unilaterali. Oggetto delle norme CBMs è quindi la raccolta e la condivisione delle informazioni e la facilitazione delle comunicazioni tra i soggetti coinvolti, pubblici o privati.

Ulteriore rilevante organizzazione regionale è l'ASEAN *Regional Forum* (ARF). Le misure proposte, in questo contesto, in materia di *cyber security* prevedono principalmente lo sviluppo di una serie di principi volti a rafforzare un comune approccio alle relazioni interstatali nell'area e l'adozione di un approccio comprensivo alla sicurezza. Tali misure, tuttavia, sembrano essere costruite sulla base di quanto elaborato in sede OSCE.

Da ultimo rileva l'attività della NATO. All'interno dell'Alleanza Atlantica le problematiche del *cyberspace* sono state oggetto di lunga discussione, a livello politico ma soprattutto a livello strategico-militare. Nel campo della *cyberwarfare* la NATO è sicuramente dotata degli strumenti tecnici e politico-istituzionali di maggior rilievo.

L'organizzazione, in seguito alla vicenda estone, ha sviluppato moltissimo la ricerca, di tipo scientifico militare, istituendo nel 2009 il NATO *Cooperative Cyber Defence Center of Excellence* (NATO CCD COE). Sul piano giuridico, all'interno delle attività di tale centro, è stato redatto un manuale sulla disciplina giuridica della guerra cyber, il *Manual on the International Law Applicable to Cyber Warfare* o *Tallinn Manual*, che rappresenta uno dei principali riferimenti scientifici in materia[12].

[12] cfr. a cura di Michael N. Schimitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* , Cambridge University Press, 2013; JAMES E. MCGHEE, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Polycy*, Journal of Law and Cyber Warfare Volume 2 Winter 2013 Issue 1; FABIO RUGGE, *Le ragioni per una rafforzata cooperazione tra NATO e UE per la protezione dello spazio cibernetico*, in *Intelligence e interesse nazionale*, a cura di UMBERTO GORI, LUIGI MARTINO, Aracne Editrice, 2015.

IV. *Direttrici dello sviluppo normativo* - L'approccio seguito dalle organizzazioni internazionali sembra orientarsi, dal punto di vista giuridico, lungo le due direttrici: sviluppo di norme CBMs, da un lato, ed applicazione delle norme di diritto internazionale relative allo *jus ad bello* e allo *jus in bello*, dall'altro.

La necessità di sviluppare entrambe le direttrici e la loro complementarietà, ai fini dell'individuazione di un quadro giuridico complessivo del *cyberspace*, è chiaramente espresso nel *Report* GGE. In esso si riconosce la necessità di determinare quali norme, procedure e principi possono essere applicate alla condotta degli Stati nel dominio *cyber*.

A tal fine un primo obiettivo prevede l'adozione di norme CBMs che possano ridurre i rischi alla pace, alla sicurezza ed alla stabilità internazionale. Secondo il *Report*, tali norme «*reflect the expectations of the International Community set standard for responsible State behavior and allow the International community to assess the activities and intention of State. Norm can help to prevent conflict to its peaceful use to enable full realization of ICTs increase global social and economic development*»[13].

Per quanto attiene alla disciplina dei conflitti interstatali il GGE, diversamente, rileva che «*the international law, and in particular the Charter of United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment*»[14].

I due insiemi normativi, rispondono ad esigenze differenti.

Lo sviluppo di principi, *standard*, procedimenti e *best practice* assolve alla funzione di delineare modi, forme e limiti dell'azione dello Stato nella sua dimensione amministrativa. Tali norme sono funzionali allo sviluppo e implementazione delle tecnologie informatiche in quanto ad esse è associato l'interesse proprio della CI allo sviluppo dell'umanità. Oggetto di tali norme, pertanto, sono i vari aspetti dell'organizzazione dei pubblici uffici coinvolti, così come le modalità e i limiti della loro azione nonché il loro rapporto con privati, cittadini o *stakeholder*. Da tali aspetti dipende infatti la diffusione e la tutela dei diritti umani nel cyberspace, la lotta al *cyber crime* nelle sue varie forme, la sicurezza dei sistemi economici e dei servizi pubblici.

Diversamente, le norme del diritto internazionale e della Carta ONU, si ritiene siano in grado di garantire il mantenimento della pace e della sicurezza internazionale anche rispetto ai conflitti che possono avvenire nel dominio *cyber*. Il GGE evidenzia come a tali finalità rispondano i principi propri del diritto internazionale contemporaneo.

V. *Principali questioni emerse in dottrina* - Il dominio *cyber* presenta delle caratteristiche tecniche che influiscono sulle dinamiche della conflittualità e delle relazioni tra gli attori

[13] cfr. cfr. Report GGE, Assemblea Generale delle Nazioni Unite, documento A 70/174.
[14] cfr. Report GGE, Assemblea Generale delle Nazioni Unite, documento A 70/174.

che in esso agiscono[15]. Ciò, sotto il profilo strettamente giuridico, determina il problema della concreta applicabilità delle norme di diritto internazionale alle fattispecie reali che possono presentarsi nel dominio *cyber*.

Su tale aspetto la dottrina giuridica, facendo proprio l'auspicio dell'Assemblea Generale delle Nazioni Unite[16] a che si affronti lo studio di tale problematica, si è concentrata, negli ultimi anni, su alcuni aspetti ritenuti di maggior rilievo, se non anche di maggior pratica utilità.

L'aumento delle tensioni internazionali sempre più spesso determinate da fatti aventi una componente informatica, ha posto l'attenzione sull'applicabilità dello *jus ad bellum* e dello *jus in bello* ai conflitti nel dominio *cyber*.

Sul punto rilevano alcune recenti pubblicazioni in cui si evidenzia, in primo luogo, l'assenza di una *lex specialis* di diritto internazionale direttamente applicabile alla materia in oggetto. Allo stesso tempo si pone il problema di comprendere se le norme generali di diritto internazionale risultino non più adeguate, in ragione dei mutamenti delle fattispecie reali apportati dallo sviluppo delle tecnologie informatiche, nonostante vi sia un generale consenso nel ritenere che le norme di diritto internazionale e della Carta ONU, siano sufficientemente flessibili da poter trovare applicazione anche a fronte delle problematiche indicate.

In particolare, l'attenzione viene posta sulle norme della Carta ONU relative al divieto della minaccia e dell'uso della forza e alle modalità di reazione dello Stato leso.

La dottrina evidenzia come le caratteristiche del cyberspace incidono: sulla possibilità di porre in essere azioni di autodifesa in ragione del difficile accertamento del soggetto responsabile; sulla possibilità che la responsabilità debba essere attribuita ad un soggetto privato e non anche ad soggetto statuale. Da altro punto di vista, esse pongano problemi rispetto alla misura che gli eventi e i loro effetti devono avere per poter giustificare il ricorso all'uso della forza. La sussistenza, ad esempio, del requisito dell'*animus aggressionis,* può infatti essere solo apparente in quanto la misura reale degli effetti prodotti da un'azione di tipo informatico, può essere determinata da più fattori tecnici alcuni dipendenti dalla infrastruttura colpita e dalla sua gestione[17].

Ulteriori aspetti su cui la dottrina ha posto attenzione, riguardano le misure che possono essere adottate nei confronti di soggetti privati stranieri, aerei o navi, il cui

[15] cfr. GIANLUCA ANSALONE, *Cyberspazio e nuove sfide*, GNOSIS, n.3, 2012; NICHOLAS TSAGOURIAS, RUSSELL BUCHAN, *Cyber Threats and International Law,* in *Security an International Law,* a cura di MARY E. FOOTER, JULIA SCHMIDT, NIGEL D. WHITE, LYDIA DAVIES-BRIGHT, Bloomsbury, 2016,

[16] cfr. Assemblea Generale delle Nazioni Unite, risoluzione 70/237.

[17] cfr. MARCO ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014; *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 85-130; HEINTZE, HANS-JOACHIM, *From Cold War to Cyber War: the evolution of the international law of peace and armed conflict over the last 25 years*, Springer, 2016; HEATHER HARRISON DINNISS, *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012; CHRISTIAN HENDERSON, *The use of cyber force: Is the jus and bellum ready?*, QIL, Zoom-in 27 (2016),p. 3-11; Emanuele Sommario, *Applyng the jus in bello in the cyber domimain: navigation between lex data e lex ferenda*, QIL,Zoom-in 27(2016), p.13-23.

utilizzo, come infrastruttura informatica, costituisca violazione delle norme internazionali. Altro argomento discusso riguarda la possibilità di attribuire ad un privato la responsabilità per violazione del divieto dell'uso della forza. Si consideri, da questo punto di vista, la relativa facilità, soprattutto economica, con cui è possibile accedere a strumenti informatici offensivi rispetto ai tradizionali armamenti. La questione giuridica riguarda l'applicabilità delle norme interstatali ad un rapporto Stato-privato.

Il tema del rapporto tra *cyberwarfare* e rispetto dei diritti umani è stato altresì trattato da differenti angolazioni. Di particolare interesse è la questione dell'identificazione dei civili quali obiettivo delle operazioni militari. Nel dominio *cyber* tale problema assume un rilievo del tutto particolare in considerazione del fatto che oggetto di un attacco informatico, soprattutto perché condotto all'interno di un conflitto di tipo asimmetrico, possono essere intere infrastrutture pubbliche quali la rete idrica e gli ospedali[18].

VI. *Il problema della Sovranità nel cyberspace* - Una questione particolarmente interessante è rappresentata dal rapporto tra il Principio di Sovranità e il cyberspace. Tale principio, come definito dall'arbitro Huber nel caso "Isola di Palmas" del 1928, ha come suo presupposto la territorialità e come suo contenuto l'esercizio di poteri di *jurisdiction*. Nel dominio *cyber*, rispetto a tale principio, si pone il problema della mancanza di confini. Viene meno il presupposto territoriale del principio di sovranità. Conseguentemente occorre comprendere in che misura il principio di sovranità trovi applicazione nel dominio *cyber*.

Sul punto la dottrina presenta posizioni differenti[19]. Alcuni affrontano il problema partendo dai caratteri propri del *cyberspace* e, dal modo in cui questo è stato idealmente inteso, giungono ad escludere l'esercizio di qualsiasi forma di autorità sullo spazio delle reti informatiche[20]. Quanti, diversamente, pongono attenzione alle dinamiche di conflittualità che possono svilupparsi, attribuiscono un ruolo centrale allo Stato territoriale e ricavano, per estensione, la disciplina della sovranità applicabile al cyberspace. Questa particolare impostazione è seguita dal *Tallinn Manual* redatto in ambito NATO. Le due posizioni, come si può notare, si collocano agli estremi del problema. Da una parte vi è la preclusione a qualsiasi forma di esercizio dei poteri pubblici, dall'altra vi è la più intensa manifestazione dell'esercizio dei poteri pubblici, l'esercizio della forza.

[18] cfr. ELIZABETH MAVROPOULOU, *Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks*, Journal of Law and Cyber Warfare, Volume 4, Spring 2015, Issue 2; GARY D. SOLIS, *The law of armed conflict: International humanitarian law in war,* Cambridge University Press, 2016; JOANNA KULESZA, ROY BALLESTE, *Cybersecurity and human rights in the age of cyberveillance,* Lanham: Rowman, Littlefield 2016.

[19] cfr. ENEKEN TIKK, *Comprehensive legal approach to cyber security,* Tartu University Press, 2011, p. 98.

[20] cfr. LAWRENCE LESSING, *Free colture*, 2004, p. xiv, disponibile su http://www.free-culture.cc/freecontent/, consultato il 14/11/2016; DAVID JOHNSON, DAVID POST, *Law Borders – the rise of law in cyberspace*, 48 Stan. L. Rev. 1367,1373, 1996.

Tuttavia l'esercizio della Sovranità e soprattutto dei poteri di *jurisdiction* ad essa inerenti, assume un ruolo fondamentale in tutte quelle situazioni che si pongono tra i due estremi indicati. La tutela delle libertà delle persone, dalla libertà di espressione al diritto alla *privacy*, il libero esercizio dell'attività economica, che costituisce uno degli elementi di base della potenza degli Stati, richiedono, per il loro sviluppo, di poter fare affidamento su regole certe e soprattutto su meccanismi di tutela giurisdizionale effettivi. La definizione di nuovi presupposti per l'esercizio della Sovranità e dei connessi poteri di *jurisdiction* assume quindi un'importanza centrale e non potrà non essere oggetto di approfonditi studi giuridici.