Istituto Affari Internazionali

Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza

di Luigi Martino

ABSTRACT

Le attività malevole condotte nel cyberspazio incidono non solo sulla sicurezza nazionale e dei cittadini, ma influenzano anche la pace e la stabilità internazionale. Per limitare il pericolo di escalation politico-militare, organizzazioni internazionali, regionali e multilaterali come le Nazioni Unite, l'Organizzazione per la Sicurezza e la Cooperazione in Europa e il G7, hanno lanciato diverse iniziative diplomatiche e normative, con l'obiettivo di migliorare la cooperazione multilaterale e aumentare la fiducia e la trasparenza tra gli stati nell'arena cyber. Una delle prime iniziative è stata lanciata dall'Onu sul finire degli anni Novanta e sulla scia della distensione internazionale seguita alla caduta del Muro di Berlino. In linea con tale iniziativa, nel 2012 l'Osce ha creato un apposito gruppo di lavoro informale volto a sviluppare un quadro di misure utili a ridurre i rischi di conflitti nel dominio cibernetico. Ma in che modo esattamente queste iniziative diplomatiche sono in grado di garantire la stabilità e la sicurezza internazionale nel cyberspazio? Quali sono i punti di forza e di debolezza principali di queste iniziative multilaterali? E quale può essere il ruolo dell'Italia in tale contesto?

Sicurezza informatica | *Politica digitale* | *Onu* | *Osce* | *G7*

keywords

IAI PAPERS 21 | 13 - MARZO 2021

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza

di Luigi Martino*

Introduzione

Il cyberspazio[1], oltre a possedere una dimensione tecnica e tecnologica, è diventato un elemento cruciale di natura politica, militare, sociale e finanziaria. La capacità delle armi cibernetiche di provocare danni reali e il conseguente utilizzo di strumenti informatici per il raggiungimento di obiettivi politico-militari è ormai un fatto incontrovertibile[2]. La conseguenza di tale combinazione di strumenti e fini ha sancito la militarizzazione del campo di battaglia cyber divenuto la "quinta dimensione della conflittualità"[3].

[1] Non esiste una definizione univoca del termine cyberspazio. In questo studio si è deciso di fare riferimento alla definizione fornita da Kuehl, ovvero "an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructures", e a quella fornita da Nye, ovvero "a unique combination of physical and virtual properties, [composto da] physical infrastructure layer [e] the virtual or informational layers". Cfr. Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", in Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz (a cura di), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 4, https://ndupress.ndu.edu/Media/News/Article/1216674; Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, Cambridge, Belfer Center for Science and International Affairs, 2014, p. 1, https://www.belfercenter.org/node/78998.

[2] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", in *International Security*, vol. 41, n. 4 (2016/17), p. 44-71, https://doi.org/10.1162/ISEC_a_00266.

[3] Luigi Martino, "La quinta dimensione della conflittualità, l'ascesa del cyberspazio e i suoi effetti sulla politica internazionale", in *Politica & Società*, n. 1 (gennaio-aprile 2018), p. 61-76. Da un punto di vista meramente politico, un numero crescente di eventi, ad es. gli attacchi cibernetici a istituzioni (private e pubbliche) in Estonia (2007), Georgia (2008), Iran (2010), Ucraina (2015-2017) e il caso del malware WannaCry (2017) – hanno dimostrato come le armi informatiche possano essere utilizzate per innescare tensioni politico-militari o persino conflitti tra stati. Questo aspetto introduce una novità sui generis: la militarizzazione del cyberspazio ha portato all'affermazione di una "quinta

* Luigi Martino insegna "ICT Policies and Cybersecurity" presso la Scuola "Cesare Alfieri" dell'Università di Firenze ed è responsabile e coordinatore del Center for Cyber Security and International Relations Studies (Ccsirs), osservatorio del Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (Cssii) presso il Dipartimento di Scienze Politiche e Sociali dell'Università di Firenze.

· Studio prodotto nell'ambito del progetto "La geopolitica del digitale", marzo 2021.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

A esacerbare tale situazione vi è la natura intrinseca degli strumenti informatici che, data la loro economicità e facilità di utilizzo, permettono l'abbassamento delle barriere di accesso alla violenza e allo stesso tempo sono del tutto indifferenti ai limiti imposti dalla geografia[4].

Queste condizioni hanno causato un "affollamento" dell'arena cyber internazionale, consentendo l'ingresso nel sistema di "attori periferici" (medie e financo piccole potenze) e il coinvolgimento di una serie di *stakeholder* che non sono più solo e soltanto i governi, ma anche attori non statali, dalle società multinazionali ai gruppi terroristici ai singoli individui[5]. Tutti questi *stakeholder* si confrontano nell'arena cyber internazionale[6].

dimensione del conflitto" dove, però, il tipo di armi non militari utilizzate per combattere, nonché i bersagli degli attacchi, fanno dei sistemi informatici (soprattutto civili) i nuovi centri di gravità per la protezione da un nemico che, il più delle volte, "agisce nell'ombra". International Institute for Strategic Studies (Iiss), "Evolution of the Cyber Domain: The Implications for National and Global Security", in *IISS Strategic Dossier*, dicembre 2015. Sulle operazioni militari nel cyberspazio, si veda, inter alia: James A. Green (a cura di), *Cyber Warfare: A Multidisciplinary Analysis*, London/New York, Routledge, 2015. Nel caso estone (2007) si è trattato di un attacco cibernetico su vasta scala che rese i principali siti internet estoni, anche quelli istituzionali, inaccessibili agli utenti con indirizzi fuori dal Paese. Secondo le autorità di Tallinn la provenienza di buona parte degli attacchi riconduceva a indirizzi IP situati in Russia. Attacchi simili sono stati subiti dalla Georgia l'anno seguente come risposta all'invasione georgiana dell'Ossezia del Sud. Il malware Stuxnet (2010) è stato usato, invece, per sabotare la centrale nucleare di Natanz in Iran, rappresentando un punto di riferimento per la verifica empirica degli effetti cinetici di un attacco cibernetico. Gli attacchi contro la rete elettrica ucraina nel dicembre 2015 hanno lasciato circa 230.000 persone nell'ovest del paese senza elettricità per ore, mentre nel 2017 i bersagli principali degli attacchi sono stati istituti bancari, ospedali ed agenzie governative. Infine, il malware WannaCry avrebbe colpito oltre un milione di sistemi unici in un attacco su scala globale, comprese le gravi implicazioni per diversi ospedali nel Regno Unito, dove ha cancellato migliaia di appuntamenti e operazioni. Sui casi riportati si vedano: Camille Marie Jackson, "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success", in *New Voices in Public Policy*, vol. 7, n. 1 (2013), http://dx.doi.org/10.13021/nvpp.v7i1.69; David Hollis, "Cyberwar Case Study: Georgia 2008", in *Small Wars Journal*, 6 gennaio 2011, https://smallwarsjournal.com/node/10080; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", in *Wired*, 3 novembre 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", in *Wired*, 3 marzo 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid; National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*, 24 ottobre 2017, https://www.nao.org.uk/?p=67469.

[4] Secondo quanto afferma Gregory J. Rattray il cyberspazio "è molto più mutevole rispetto ad altri ambienti; a differenza delle montagne e degli oceani statici, le parti del cyberspazio possono essere attivate e disattivate con un semplice click". Gregory J. Rattray, "An Environmental Approach to Understanding Cyberspace", in Franklin Kramer, Stuart H. Starr e Larry K. Wentz (a cura di), *Cyberpower and National Security*, cit., p. 256.

[5] William J. Lynn III, "Defending a New Domain", in *Foreign Affairs*, vol. 89, n. 5 (2010), p. 97-108.

[6] Si vedano: Kenneth Geers et al., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, Milpitas, FireEye, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf; Michael N. Schmitt e Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", in *Fletcher Security Review*, vol. 1, n. 2 (2014), p. 55-73, https://059927f5-49c6-47fa-92e9-3d499a0e6da2.filesusr.com/ugd/c28a64_2610a29ebee34169988ab7a3d7c7412e.pdf.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Allo stesso tempo, le tecnologie dell'informazione e della comunicazione (Ict) hanno aumentato notevolmente il rischio di percezioni errate tra gli Stati, soprattutto in relazione a questioni di intenzionalità, atteggiamento, responsabilità, regole e norme internazionali[7]. In altre parole, si è venuta a creare una pericolosa instabilità: la mancanza di un quadro diplomatico, normativo e giuridico che garantisca delle "regole del gioco" condivise[8].

Un problema di grande rilevanza è, ad esempio, la difficoltà di attribuire gli attacchi informatici "al di là di ogni ragionevole dubbio", condizione che rende possibile negare la responsabilità (c.d. *plausible deniability*[9]) con il conseguente indebolimento dei tentativi di avviare un dialogo a livello internazionale basato sulla fiducia reciproca e sulla trasparenza[10].

La consapevolezza dei rischi e delle minacce derivanti dall'uso malevolo degli strumenti informatici ha spinto le organizzazioni internazionali e regionali a lanciare iniziative multilaterali per rafforzare la cooperazione e aumentare la fiducia e la trasparenza, con l'obiettivo di definire norme di comportamento responsabile degli stati nel cyberspazio[11]. In altre parole, raggiunta la consapevolezza che il cyberspazio può produrre effetti destabilizzanti, la comunità internazionale ha deciso di avviare i lavori per la costituzione di una cornice di *cyber diplomacy* che può essere definita, come l'uso di risorse diplomatiche e lo svolgimento di funzioni diplomatiche per tutelare gli interessi nazionali rispetto al cyberspazio e garantire strumenti utili per evitare o limitare le crisi politico-militari[12].

La necessità di valorizzare la cooperazione internazionale nel contesto cyber è riconosciuta anche dall'Italia nell'indirizzo strategico n. 6 del "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" che stabilisce il "rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica nell'ambito

[7] Tim Maurer e Jason Healey, "What It'll Take to Forge Peace in Cyberspace", in *The Christian Science Monitor*, 20 marzo 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/What-it-ll-take-to-forge-peace-in-cyberspace; Luigi Martino, "La quinta dimensione della conflittualità...", cit.; Ronald J. Deibert e Rafal Rohozinski, "Under Cover of the Net: The Hidden Governance Mechanisms of Cyberspace", in Anne L. Clunan e Harold A. Trinkunas (a cura di), *Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty*, Stanford, Stanford University Press, 2010, p. 255-272.

[8] Luigi Martino, "Cyberspace and International Relations: Diplomatic Initiatives to Avoid the Risk of Escalation in the Cyber Arena", in *European Cybersecurity Journal*, vol. 3, n. 3 (2017), p. 53-57, https://app.box.com/s/50ihrqcz29phrme0nhc1h9a6tjpwzkfv.

[9] Eva-Nour Repussard, "There Is No Attribution Problem, Only a Diplomatic One", in *E-International Relations*, 22 marzo 2020, https://www.e-ir.info/?p=82357.

[10] Luigi Martino, "Cyberspace and International Relations...", cit.

[11] Paul Meyer, "Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda", in *The RUSI Journal*, vol. 157, n. 1 (febbraio 2012), p. 14-19.

[12] La tutela di questi interessi viene di solito identificata nelle strategie nazionali sulla sicurezza informatica o sull'uso del cyberspazio, che includono riferimenti al posizionamento internazionale dello Stato. Si veda: André Barrinha e Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age", in *Global Affairs*, vol. 3, n. 4-5 (dicembre 2017), p. 353-365, https://doi.org/10.1080/23340460.2017.1414924.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

delle Organizzazioni di cui l'Italia è membro e con i Paesi alleati"[13].

Alla luce di quanto descritto sopra, questo studio si pone dunque l'obiettivo di delineare le iniziative diplomatiche avviate a livello internazionale, regionale, multilaterale e bilaterale mettendone in evidenza i limiti, gli ostacoli e i punti di forza della loro implementazione. Il lavoro è suddiviso in tre parti. La prima propone una rassegna delle maggiori iniziative diplomatiche implementate a livello internazionale, regionale, multilaterale e bilaterale. Nella seconda parte viene condotta un'analisi critica di queste, mettendo in evidenza ostacoli e sfide delle iniziative di *cyber diplomacy*. Infine, sulla base degli elementi emersi, l'ultima parte affronta in maniera sistematica i punti di forza e di debolezza delle iniziative diplomatiche per la stabilità nel cyberspazio anche in riferimento a un possibile ruolo dell'Italia.

1. Iniziative diplomatiche di mitigazione del rischio di escalation politico-militare nel cyberspazio

Riconoscendo l'urgenza di affrontare le potenziali tensioni derivanti dalle azioni malevole prodotte nel dominio cibernetico, la comunità internazionale ha iniziato a esplorare azioni diplomatiche utili per garantire la pace e la stabilità internazionale[14].

La tabella 1 riassume le principali iniziative diplomatiche implementate per favorire la cooperazione nel cyberspazio a livello internazionale e regionale[15].

Come emerge dalla tabella 1, la prima iniziativa diplomatica è stata lanciata all'interno della cornice delle Nazioni Unite (Onu). Nel 1998, infatti, su proposta della Russia, l'Assemblea Generale ha approvato la risoluzione 53/70 al fine di valutare i meccanismi per mitigare i rischi causati dall'uso malevolo delle tecnologie informatiche e migliorare così la cooperazione internazionale nel

[13] Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, p. 19, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf. L'indirizzo strategico si traduce nell'indirizzo operativo n. 4 che afferma il "rafforzamento dei rapporti di cooperazione e collaborazione con le Organizzazioni internazionali delle quali l'Italia è parte, con i Paesi alleati e con le Nazioni amiche; partecipazione attiva del Paese alle iniziative e ai fora internazionali di trattazione della materia" a livello globale, europeo, atlantico e bilaterale. Ibid., p. 21-22. Si veda anche: Presidenza del Consiglio dei ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, marzo 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[14] Si veda il sito United Nations Office for Disarmament Affairs (Unoda): *Open-ended Working Group*, https://www.un.org/disarmament/open-ended-working-group.

[15] La tabella contiene solo alcune principali iniziative a livello internazionale e regionale ed è stata elaborata dall'autore secondo i dati ripresi da Deborah Housen-Couriel, "An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives", in Global Commission on the Stability of Cyberspace, *Briefings from the Research Advisory Group*, New Delhi, novembre 2017, p. 39-74, https://cyberstability.org/?p=792.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

cyberspazio[16]. Dopo l'adozione della risoluzione, l'Assemblea Generale ha istituito un gruppo di esperti governativi sugli sviluppi nel campo dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale (Gge) che, dal 2004, si è posto come obiettivo principale lo studio delle minacce e delle sfide alla sicurezza internazionale derivanti dal cyberspazio, con il fine di proporre azioni utili per migliorare la stabilità e la cooperazione internazionale[17].

Tabella 1 | Principali iniziative diplomatiche per la stabilità e la cooperazione nel cyberspazio a livello internazionale e regionale

Organizzazione		Documento	Data	Status
Onu	UN Group of Governmental Experts (Gge)	Reports on developments in the field of information and telecommunications in the context of international security	2010 2013 2015 2017	Approvato Approvato Approvato Nessun consenso
	UN Open-Ended Working Group (Oewg)	Final substantive report	2021	Approvato
Osce	Informal Working Group (Iwg)	Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies	2013 2016	Adottato Adottato
G7	Ise-Shima Cyber Group	Principles and actions on cyber declaration on responsible state behavior in cyberspace	2016 2017	Adottato Adottato

Nota: iniziative su base volontaria.
Fonte: analisi empirica condotta dall'autore in base alle informazioni e ai dati raccolti open-source.

Ad esempio, il rapporto del 2013 raccomandava di porre le basi per lo sviluppo di: "norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space" [norme, regole o principi del comportamento responsabile degli Stati e misure di rafforzamento della fiducia riguardo allo spazio dell'informazione][18]. Nel rapporto del 2015 il Gge ha indicato tra le principali priorità la necessità di approfondire l'analisi dell'applicabilità del

[16] UN General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/53/70), 4 dicembre 1998, http://undocs.org/A/RES/53/70.

[17] Per una breve panoramica cronologica del gruppo di lavoro si veda il sito GIP Digital Watch: *UN GGE and OEWG*, https://dig.watch/processes/un-gge. Sul suo lavoro si veda: UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201), 30 luglio 2010, http://undocs.org/A/65/201.

[18] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98), 24 giugno 2013, http://undocs.org/A/68/98.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

diritto internazionale esistente anche al dominio cyber e la necessità di fornire misure per costruire la fiducia, trasparenza e cooperazione tra stati[19]. Tuttavia, i limiti principali del Gge sono stati essenzialmente due: 1) il carattere volontario di implementazione delle norme da parte degli Stati e, 2) la difficoltà di saper adeguare le discussioni interne al gruppo di lavoro in base al mutamento del contesto geopolitico, come dimostrato, ad esempio, nel caso degli attacchi cibernetici subiti dall'Ucraina nel 2015[20]. A tali limiti si aggiunge anche l'immagine di "club esclusivo" dovuta alla mancanza di inclusività non solo di molti Stati, ma soprattutto degli attori non statali, nel processo decisionale del Gge[21].

Tuttavia, seppure con evidenti limiti di efficacia, in questo quadro di iniziative promosse dalle Nazioni Unite va inserita soprattutto l'azione efficiente svolta dall'Organizzazione per la Sicurezza e la Cooperazione in Europa (Osce)[22] ritenuta da molti osservatori come un valido modello di *cyber diplomacy* e basata essenzialmente sull'adozione di misure di rafforzamento della fiducia (*confidence building measures*, Cbm) nel cyberspazio[23].

L'iniziativa ha avuto inizio attraverso l'istituzione di un gruppo di lavoro informale (*Informal Working Group*, Iwg) volto a discutere le dinamiche del dominio cibernetico al fine di innalzarne la stabilità e la sicurezza all'interno dell'Osce. L'obiettivo principale è stato quello di verificare l'adattabilità del quadro delle Cbm all'ambiente cibernetico, partendo dal presupposto che l'approccio delle Cbm si è già dimostrato efficace come meccanismo di prevenzione delle crisi durante la Guerra Fredda[24].

[19] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), 22 luglio 2015, http://undocs.org/A/70/174.

[20] Christian Ruhl et al., "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads", in *Carnegie Working Papers*, febbraio 2020, https://carnegieendowment.org/publications/81110.

[21] Ibid.

[22] Il vantaggio specifico dell'avvio di questo processo all'interno dell'Osce è essenzialmente dovuto all'approccio globale e inter-dimensionale dell'organizzazione basato sui suoi principi fondamentali e sulla sua tradizione di foro per la cooperazione internazionale. L'Osce ha tenuto il suo 19° Consiglio ministeriale il 6-7 dicembre 2012 a Dublino, in cui ha discusso la sicurezza informatica e le Cbm. La proposta di un'allerta specifica al fine di notificare in anticipo le operazioni degli Stati nel dominio cibernetico (in particolare per quanto riguarda le attività militari) è fallita a causa della mancanza di consenso tra gli Stati partecipanti.

[23] Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in Anna-Maria Osula e Henry Rõigas (a cura di), *International Cyber Norms: Legal Policy and Industry Perspectives*, Tallinn, NATO CCD COE Publications, 2016, p. 129-153 (capitolo 7), https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives. L'approccio Cbm si è dimostrato un meccanismo efficace per prevenire le crisi politico-militari durante l'era della Guerra Fredda, stabilendo linee rosse effettive tra gli Stati Uniti e l'Urss. In altre parole, "such measures are designed to resolve crises and conflicts, and to support a more accurate and reciprocal assessment of matters related to mutual security". Iiss, "Evolution of the Cyber Domain...", cit.

[24] Patryk Pawlak, "Confidence-Building Measures in Cyberspace...", cit.

IAI PAPERS 21 | 13 - MARZO 2021

ISSN 2610-9603 | ISBN 978-88-9368-187-2

In particolare, in quanto "attività principale" dell'Osce, l'approccio Cbm è in grado di "stabilire il livello di aspettativa sul comportamento degli Stati nel cyberspazio" con lo scopo di migliorare la stabilità e incoraggiare la fiducia, la cooperazione e la trasparenza tra gli Stati[25].

Nel 2013 i 57 stati membri dell'Osce hanno approvato le prime Cbm (11 in totale) incentrate principalmente sulla creazione di misure di trasparenza, canali di comunicazione e fiducia tra gli stati. Nel 2016 è stata approvata una seconda serie di Cbm (cinque in totale) con la definizione di un primo (e attualmente l'unico) quadro di misure "non vincolanti" a livello internazionale[26].

Anche le iniziative implementate in sede Osce hanno risentito del clima di tensione politica e ideologica scaturito in seno al Gge, il che ha portato alla sospensione dell'iter di approvazione del terzo set di Cbm Osce interamente dedicato al "come" applicare il diritto internazionale esistente al dominio cyber[27].

Tale clima di tensione ha esacerbato il dialogo all'interno delle Nazioni Unite su tali tematiche a tal punto che nel 2018, tramite la risoluzione 73/27 dell'Assemblea Generale delle Nazioni Unite su proposta della Federazione Russa è stato istituito un gruppo di lavoro aperto (*Open-Ended Working Group*, Oewg), a cui tutti i membri delle Nazioni Unite sono stati invitati a partecipare[28]. Il primo messaggio dunque è stato quello di superare l'approccio di "club esclusivo" del Gge (dal quale era esclusa anche l'Italia), garantendo una maggiore rappresentatività tramite l'Oewg.

Quest'ultimo foro ha come compito principale quello di continuare a sviluppare regole, norme e principi di comportamento responsabile degli Stati, discutendo le modalità per la loro attuazione e la possibilità di stabilire un dialogo istituzionale sotto gli auspici dell'Onu.

Sebbene l'Oewg sia ancora un processo *in fieri*, sulla base del lavoro svolto dal Gge il nuovo gruppo, che ha coinvolto anche il settore privato e la società civile, ha messo a punto un documento preliminare che ha riconosciuto il ruolo delle Cbm nel creare "fiducia e stabilità nelle relazioni tra gli Stati". L'approccio indicato in questa rapporto, approvato con largo consenso nel marzo 2021, si basa sulla consapevolezza della minaccia cyber, sull'applicabilità delle norme di diritto internazionale e sul rafforzamento della fiducia nel cyberspazio attraverso l'adozione volontaria delle Cbm e la cooperazione per la loro attuazione[29].

[25] Ibid.

[26] Osce, *Permanent Council Decision No. 1202*, 10 marzo 2016, https://www.osce.org/pc/227281.

[27] Si veda Patryk Pawlak, "Confidence-Building Measures in Cyberspace…", cit.

[28] Il processo ha previsto, quindi, riunioni consultive con l'industria, le organizzazioni non governative e il mondo accademico. Si veda il sito Unoda: *Open-ended Working Group*, cit.

[29] Ibid.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

2. Ostacoli e sfide delle principali iniziative di *cyber diplomacy*

I processi guidati dalle Nazioni Unite hanno quindi dedicato attenzione alla questione delle norme di comportamento responsabile nel cyberspazio. Alcune delle norme adottate nei rapporti Gge e nella Risoluzione che istituisce l'Oewg sono radicate nelle norme e nei principi esistenti del diritto internazionale; altre forniscono ulteriori indicazioni su come interpretare gli obblighi giuridicamente vincolanti a livello internazionale esistenti[30]. In particolare, il rapporto Gge del 2015 ha evidenziato il ruolo di norme volontarie di comportamento responsabile degli stati per la riduzione del rischi alla pace e alla sicurezza internazionale. In questo senso, dal punto di vista delle previsioni normative e del richiamo all'applicabilità del diritto internazionale nel cyberspazio, si raccomanda che uno Stato non conduca o sostenga operazioni nel cyberspazio che possano essere contrarie ad obblighi di diritto internazionale, danneggiando ad esempio, le infrastrutture critiche o compromettendone il funzionamento e la fornitura dei servizi essenziali.

Un altro richiamo riguarda la limitazione delle operazioni nel cyberspazio che possano danneggiare le squadre di risposta rapida (*computer emergency response team*, Cert) o, altrimenti, usarli per condurre azioni malevole. In queste due limitazioni è presente un chiaro riferimento al diritto internazionale umanitario, in particolare riguardo all'obbligo di prendere tutte le misure utili al fine di evitare che i civili possano diventare obiettivi di attacchi nonché dello status speciale di protezione del personale medico, qui esteso ai Cert[31]. Un'ultima raccomandazione concerne la maggiore condivisione delle informazioni fra Stati sulle vulnerabilità nel cyberspazio. Tuttavia, nonostante la condivisione politica su tali principi, il crescente utilizzo di strumenti cyber per fini politici militari, ha dimostrato che le raccomandazioni si scontrano con il carattere volontaristico delle norme e con le tensioni di carattere geopolitico[32].

Allo stesso tempo è emerso come la necessità di un quadro giuridicamente vincolante resti tuttavia una questione controversa. Ad esempio alcuni stati, come la Russia e la Cina, continuano a mettere in dubbio l'adeguatezza dell'attuale diritto

[30] Queste norme, tuttavia, non fanno alcun riferimento esplicito alle regole o ai principi del diritto internazionale da cui derivano. Nel già citato rapporto del 2015 del Gge (A/70/174), ad esempio, la norma 13 (c) stabilisce che: "Gli Stati non dovrebbero consapevolmente consentire che il loro territorio sia utilizzato per atti internazionalmente illeciti utilizzando le tecnologie Ict". È una chiara interpretazione del principio di due diligence nel regno cibernetico.

[31] Paul Meyer, "Norms of Responsible State Behaviour in Cyberspace", in Markus Christen, Bert Gordijn e Michele Loi (a cura di), *The Ethics of Cybersecurity*, Cham, Springer, 2020, p. 247-360, https://doi.org/10.1007/978-3-030-29053-5_18.

[32] In questa prospettiva, il World Economic Forum ha classificato gli attacchi informatici come il nono rischio globale più probabile per il 2021. World Economic Forum, *The Global Risks Report 2021*, gennaio 2021, https://www.weforum.org/reports/the-global-risks-report-2021. Per una panoramica della crescente tendenza degli attacchi informatici che coinvolgono scopi "politici", si veda il "Cyber Operations Tracker" del Council on Foreign Relations che raccoglie gli attacchi sponsorizzati da Stati, disponibile all'indirizzo: https://www.cfr.org/interactive/cyber-operations.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

internazionale con la proposta di nuove norme adeguate al contesto cyber[33].

Non è un caso se, secondo alcuni autori, le divisioni palesate dal processo in seno all'Oewg potrebbero aumentare la confusione tra regole e principi del diritto internazionale e norme non vincolanti. Infatti, l'assenza di riferimenti chiari all'applicabilità del diritto internazionale nel cyberspazio potrebbe aumentare le difficoltà di interpretazione, alimentando interpretazioni incoerenti od opposte[34].

In questo senso è possibile sostenere l'ipotesi che il percorso verso un solido quadro normativo internazionale si è conseguentemente indirizzato verso lo scambio di buone pratiche e, come visto, verso una maggiore integrazione del contributo delle organizzazioni regionali e delle loro interpretazioni delle norme che si riferiscono, nel caso specifico al concetto e alla pratica della stabilità nel cyberspazio. Come emerso dall'analisi dalle azioni implementate dall'Osce[35] le iniziative diplomatiche in questo settore possono contribuire indirettamente a promuovere le attività di altre organizzazioni regionali e sub-regionali. Lo dimostra ad esempio quanto avviene nell'Asean Regional Forum (che raccoglie i paesi del Sudest asiatico membri dell'Asean più Cina, Giappone e Corea del Sud), nel contesto dei paesi Brics (Brasile, Russia, India, Cina e Sud Africa), nel Comunità degli Stati Indipendenti (Cis, i cui membri sono quasi tutte le ex repubbliche sovietiche), nell'Organizzazione degli Stati americani (Oas) e nell'Organizzazione per la cooperazione di Shanghai (Sco). Tutte queste organizzazioni hanno identificato le Cbm come importanti strumenti per garantire una maggiore cooperazione e capaci di rafforzare la stabilità e la sicurezza nel cyberspazio[36].

Pur concentrandosi principalmente sullo sviluppo economico, la stabilità commerciale e finanziaria, l'Organizzazione per la cooperazione e lo sviluppo economico (Ocse), il G20 e l'International Organization of Securities Commissions (Iosco) hanno anche identificato le Cbm e il lavoro svolto dall'Osce come azioni

[33] ICT4Peace, *Second Substantive Session of the UN Negotiations on Cybersecurity*, 6 marzo 2020, https://ict4peace.org/?p=14223. Si veda anche UN General Assembly, *Resolution adopted by the General Assembly on 5 December 2018* (A/RES/73/27), 11 dicembre 2018, https://undocs.org/A/RES/73/27. Nel 2019 la Federazione Russa ha poi proposto un gruppo di lavoro aperto allo scopo di evitare la creazione di accordi esclusivi e di incoraggiare un processo di negoziazione inclusivo e aperto, promuovendo la costruzione di norme condivise e il rafforzamento della fiducia tra gli Stati. Questa posizione non è stata sostenuta dalla delegazione degli Stati Uniti, che accusa la Russia di aver "selezionato con cura" e riformulato passaggi di precedenti documenti del Gge. In effetti, la risoluzione di tre pagine guidata dagli Stati Uniti sottolinea con forza l'importanza e la necessità di un ecosistema aperto, affidabile e sicuro, coerente con la necessità di preservare il libero flusso di informazioni.

[34] Si veda François Delerue, Xymena Kurowska e Patryk Pawlak, *Reflections on the Pre-draft of the Report of the OEWG on Developments in the Field of ICTs in the Context of International Security*, Bruxelles, EU Cyber Direct, aprile 2020, https://eucyberdirect.eu/?p=2857.

[35] Luigi Martino, *Confidence Building Measures (C.B.M.) in campo Cyber: Attuali limiti e possibile contributo nazionale alla loro condivisione e applicazione*, Roma, Centro Militare di Studi Strategici, 2019, https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/AN_UG_01.aspx.

[36] Cfr. la sezione del sito del Centro Universitario di Studi Strategici Internazionali e Imprenditoriali: *DiploInCyber*, https://www.cssii.unifi.it/vp-162-diploincyber.html.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

indispensabili per rafforzare pace e sicurezza e per realizzare il pieno potenziale delle Ict al fine di aumentare lo sviluppo sociale ed economico e la stabilità a livello globale, ridurre le disuguaglianze e contribuire all'agenda sulla trasformazione digitale[37].

Tra le iniziative extra-Onu va segnalata l'azione in materia di sicurezza del cyberspazio da parte del G7. Nel 2016 è stato creato l'Ise-Shima Cyber Group (Iscg), un tavolo permanente interamente dedicato alle tematiche cyber[38]. L'Iscg si è riunito per la prima volta nel 2017 durante il G7 presieduto dall'Italia, con l'obiettivo di stabilire "norme di comportamento responsabile dello Stato nel cyberspazio" in linea con le disposizioni del Gge delle Nazioni Unite[39]. La Dichiarazione di Lucca ha riconosciuto il ruolo predominante degli stati nel processo di costruzione di un ambiente cyber più sicuro e stabile e la validità del diritto internazionale esistente anche per il dominio cibernetico.

In altre parole, il lavoro svolto dall'Iscg del G7 (sotto la presidenza italiana) ha cercato di sottolineare la necessità di passare da un approccio prevalentemente tecnico (come avviene attualmente all'Onu dove Gee e Oewg possono solo formulare raccomandazioni) a un processo politico-diplomatico al fine di sviluppare un primo quadro di regole di condotta condivise per il cyberspazio[40].

[37] Luigi Martino, *Confidence Building Measures (C.B.M.) in campo Cyber...*, cit.

[38] Ministry of Foreign Affairs of Japan, *First Meeting of G7 "Ise-Shima Cyber Group (ISCG)"*, 14 ottobre 2016, https://www.mofa.go.jp/fp/nsp/press3e_000073.html.

[39] G7, *Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 aprile 2017, http://www.g7.utoronto.ca/foreign/170411-cyberspace.html.

[40] Anche l'approccio dell'Ue si inserisce nel riconoscimento dell'applicabilità del diritto internazionale nel cyberspazio e nella forza delle misure regionali di rafforzamento della fiducia. In questa prospettiva, nel giugno 2017 il Consiglio europeo ha deciso di sviluppare un quadro per una risposta diplomatica congiunta dell'Unione europea alle attività informatiche malevole. Ne è seguita la definizione di un *Cyber Diplomacy Toolbox* il quale si basa sulla capacità di aumentare i costi di esecuzione degli attacchi informatici, scoraggiando così i potenziali aggressori, attraverso un sistema sanzionatorio condiviso tra gli Stati membri. Questo quadro condiviso mira anche a favorire la cooperazione e ad influenzare il comportamento nel lungo periodo di possibili attori malevoli per assicurare un cyberspazio aperto, stabile e sicuro. Tuttavia le difficoltà di attribuzione rappresentano una sfida chiave nella pianificazione delle sanzioni e, quindi, di questo tipo di iniziative di *cyber diplomacy*. Inoltre, eventuali prove sull'attribuzione in base a materiale di intelligence potrebbero persino complicarne l'uso per un regime sanzionatorio in quanto si potrebbero diffondere informazioni sensibili sulle fonti o gli strumenti usati per raccogliere tali prove. Oltre ai forum internazionali e alle organizzazioni regionali, gli stati interagiscono sulle questioni cyber anche a livello bilaterale (come il dialogo Usa-Cina). Il livello bilaterale, come l'accordo tra Cina e Russia del 2015, rappresenta dal lato dell'attore statale lo strumento concreto per affrontare in maniera congiunta le minacce, creando canali di comunicazione state-to-state per una risposta efficace e immediata, attraverso lo scambio di informazioni tra i rispettivi servizi di intelligence. Si vedano: Michael N. Schmitt e Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", in *Just Security*, 30 giugno 2017, https://www.justsecurity.org/42768; Consiglio dell'Unione europea, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*, Bruxelles, 9 ottobre 2017, https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf; Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* (JOIN/2013/1), 7 febbraio 2013, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52013JC0001. Sulla questione dell'attribuzione, infine, si vada: Nigel Inkster, *China's Cyber Power*, London/New York, Routledge, 2016.

ISSN 2610-9603 | ISBN 978-88-9368-187-2

3. Punti di forza e di debolezza delle iniziative diplomatiche per la stabilità nel cyberspazio e possibile ruolo dell'Italia

Dall'analisi sullo stato di avanzamento dell'attuazione delle Cbm da parte degli Stati membri dell'Osce è emerso come queste iniziative appartengano a due campi principali: a) trasparenza e b) misure di cooperazione. A livello di trasparenza, le Cbm incoraggiano gli stati a condividere le informazioni per comprendere il loro posizionamento nell'arena informatica al fine di migliorare la prevedibilità del comportamento nel cyberspazio. Per quanto riguarda le misure di cooperazione, invece, le Cbm hanno lo scopo principale di aumentare le iniziative di dialogo attraverso la condivisione di informazioni e canali di comunicazione al fine di evitare il rischio di errata percezione (*misperception*) e, quindi, di escalation militare e politica nel cyberspazio.

L'attuale frammentazione del sistema normativo e dei processi diplomatici in parte deriva dalla preferenza degli Stati per fora ristretti più in linea con i loro interessi. Per esempio, in seguito a una serie di attacchi cibernetici (probabilmente di origine russa) l'Ucraina ha preferito rivolgersi agli Stati Uniti e alla Nato invece che utilizzare i meccanismi di risoluzione delle crisi implementati in seno all'Osce, di cui è Stato partecipante (come la Russia)[41]. Questo approccio potrebbe in parte spiegare il fallimento del Gge 2017, dove uno degli ostacoli al consenso è stato dovuto, secondo alcuni osservatori, all'espansione del gruppo a venticinque esperti, con il conseguente aumento delle difficoltà a trovare un consenso comune provocando quindi, l'indebolimento della capacità di passare dai negoziati all'implementazione delle norme[42]. In questo senso è possibile dunque concludere che la maggiore criticità delle iniziative diplomatiche nel cyberspazio è dovuta al fatto che queste sono soggette a condizionamenti (geo)politici e quindi tendono a rivelarsi inefficienti[43].

Le caratteristiche intrinseche del dominio cibernetico, come la continua evoluzione tecnologica, la mancanza di quadri normativi capaci di attribuire l'*accountability* dei produttori di strumenti tecnologici non sicuri, il conseguente adattamento delle minacce e dei rischi pongono di per sé già dei limiti allo sviluppo di processi diplomatici efficaci[44]. La trasparenza sui comportamenti degli Stati viene minata anche dal segreto che avvolge le operazioni cibernetiche portate avanti dagli apparati di intelligence o militari. Questo rende ancor più complesso il processo di identificazione di norme che si basano su effettive aspettative di comportamento responsabile.

[41] Luigi Martino, "Cyberspace and International Relations...", cit.
[42] Christian Ruhl et al., "Cyberspace and Geopolitics...", cit.
[43] Luigi Martino, *Confidence Building Measures (C.B.M.) in campo Cyber...*, cit.
[44] Luigi Martino, "La quinta dimensione della conflittualità...", cit..

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Infine, come sopra delineato, le posizioni divergenti degli Stati su concetti fondamentali come la sovranità nel cyberspazio sono alimentate da processi frammentati (del tipo *multiple-layers*) delle iniziative diplomatiche stesse.

Conclusioni

Nonostante stiamo assistendo al consolidamento del campo di battaglia cyber, delle armi cyber e dei molteplici attori, oggi mancano gli strumenti che permettono di definire delle "regole del gioco" condivise nello spazio cibernetico, un elemento essenziale per prevenire il rischio di escalation politico-militare.

La militarizzazione del cyberspazio, ufficialmente decretata dal vertice Nato di Varsavia nel 2016[45] ma *de facto* sanzionata nell'ultimo decennio da varie dottrine militari e strategie nazionali di cybersecurity, ha tolto ogni dubbio sull'intenzione degli Stati di considerare il cyberspazio come una sfera piegata ai conflitti militari, anche se quest'area è stata originariamente creata con caratteristiche puramente tecnologiche[46].

Sulla scia di raccomandazioni adottate nella cornice delle Nazioni Unite (in particolare in ambito Gge), l'Osce è stata la prima organizzazione regionale ad approvare una serie di misure con l'obiettivo di ridurre il rischio che un utilizzo malevolo degli strumenti informatici possa minare la stabilità internazionale.

Tuttavia, sebbene questo processo sia legittimato dal consenso unanime degli Stati partecipanti che hanno sancito l'approvazione di sedici Cbm, in pratica l'azione dell'Osce richiedeva e richiede tutt'ora uno specifico "piano d'azione" al fine di permettere una ricaduta pratica di tali iniziative[47]. Tale processo è stato interrotto dalle tensioni politiche, prevalentemente tra Russia e Stati Uniti. Tuttavia, come dimostrato dalle iniziative del Gge, dell'Osce, del G7 e dell'Oewg è possibile avviare un processo politico di *cyber diplomacy* capace di trasformare un consenso politico in una pratica diffusamente riconosciuta che, date determinate condizioni, può portare alla creazione di norme consuetudinarie.

In questa prospettiva, per il caso specifico italiano, è possibile porre le basi, in continuità con la Dichiarazione di Lucca e nel rafforzamento delle Cbm proposte

[45] Come sottolineato dal Segretario Generale della Nato nel 2019, un attacco cibernetico contro uno Stato membro potrebbe innescare il meccanismo di difesa collettiva previsto dall'art. 5. Si vedano: Jens Stoltenberg, "NATO Will Defend Itself", in *Prospect*, ottobre 2019, p. 4, https://www.nato.int/cps/en/natohq/news_168435.htm; NATO Cooperative Cyber Defence Centre of Excellence, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, 21 luglio 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit.

[46] Michael N. Schmitt e Liis Vihul, "Proxy Wars in Cyberspace...", cit.

[47] UN General Assembly, "Draft Guidelines for Appropriate Types of Confidence-Building Measures and for the Implementation of Such Measures on a global or Regional Level", Annex II in *Report of the Disarmament Commission* (A/41/42), 23 giugno 1986, https://undocs.org/A/41/42(supp).

ISSN 2610-9603 | ISBN 978-88-9368-187-2

dall'Osce, per attività regionali che promuovano il dialogo e alimentino, così, la fiducia reciproca tra gli Stati. Questo tipo di attività deve essere, allo stesso tempo, accompagnato da linee guida e strumenti per supportare l'implementazione di misure specifiche a livello nazionale – in particolare in quei contesti in cui competenze e risorse sono più fragili e incerte – attraverso appositi programmi di *capacity building*. L'azione di *capacity building* potrebbe rivolgersi sia all'interno del Sistema Paese tramite l'innalzamento della competenze nazionali e della cultura della *cybersecurity*, che all'esterno attraverso attività di formazione del tipo *training of trainers* a livello politico, strategico e operativo, oltre che alla creazione di una cornice legale condivisa con i paesi *like minded* che porti all'effettiva capacità di mitigare i rischi cyber e garantire la pace e la stabilità internazionale.

aggiornato 26 marzo 2021

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Riferimenti

André Barrinha e Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age", in *Global Affairs*, vol. 3, n. 4-5 (dicembre 2017), p. 353-365, https://doi.org/10.1080/23340460.2017.1414924

Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* (JOIN/2013/1), 7 febbraio 2013, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52013JC0001

Consiglio dell'Unione europea, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*, Bruxelles, 9 ottobre 2017, https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Ronald J. Deibert e Rafal Rohozinski, "Under Cover of the Net: The Hidden Governance Mechanisms of Cyberspace", in Anne L. Clunan e Harold A. Trinkunas (a cura di), *Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty*, Stanford, Stanford University Press, 2010, p. 255-272

François Delerue, Xymena Kurowska e Patryk Pawlak, *Reflections on the Pre-draft of the Report of the OEWG on Developments in the Field of ICTs in the Context of International Security*, Bruxelles, EU Cyber Direct, aprile 2020, https://eucyberdirect.eu/?p=2857

G7, *Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 aprile 2017, http://www.g7.utoronto.ca/foreign/170411-cyberspace.html

Kenneth Geers et al., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, Milpitas, FireEye, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

James A. Green (a cura di), *Cyber Warfare: A Multidisciplinary Analysis*, London/New York, Routledge, 2015

David Hollis, "Cyberwar Case Study: Georgia 2008", in *Small Wars Journal*, 6 gennaio 2011, https://smallwarsjournal.com/node/10080

Deborah Housen-Couriel, "An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives", in Global Commission on the Stability of Cyberspace, *Briefings from the Research Advisory Group*, New Delhi, novembre 2017, p. 39-74, https://cyberstability.org/?p=792

ICT4Peace, *Second Substantive Session of the UN Negotiations on Cybersecurity*, 6 marzo 2020, https://ict4peace.org/?p=14223

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Nigel Inkster, *China's Cyber Power*, London/New York, Routledge, 2016

International Institute for Strategic Studies (Iiss), "Evolution of the Cyber Domain: The Implications for National and Global Security", in *IISS Strategic Dossier*, dicembre 2015

Camille Marie Jackson, "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success", in *New Voices in Public Policy*, vol. 7, n. 1 (2013), http://dx.doi.org/10.13021/nvpp.v7i1.69

Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", in Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz (a cura di), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 3-23, https://ndupress.ndu.edu/Media/News/Article/1216674

William J. Lynn III, "Defending a New Domain", in *Foreign Affairs*, vol. 89, n. 5 (2010), p. 97-108

Luigi Martino, *Confidence Building Measures (C.B.M.) in campo Cyber: Attuali limiti e possibile contributo nazionale alla loro condivisione e applicazione*, Roma, Centro Militare di Studi Strategici, 2019, https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/AN_UG_01.aspx

Luigi Martino, "Cyberspace and International Relations: Diplomatic Initiatives to Avoid the Risk of Escalation in the Cyber Arena", in *European Cybersecurity Journal*, vol. 3, n. 3 (2017), p. 53-57, https://app.box.com/s/50ihrqcz29phrme0nhc1h9a6tjpwzkfv

Luigi Martino, "La quinta dimensione della conflittualità, l'ascesa del cyberspazio e i suoi effetti sulla politica internazionale", in *Politica & Società*, n. 1 (gennaio-aprile 2018), p. 61-76

Tim Maurer e Jason Healey, "What It'll Take to Forge Peace in Cyberspace", in *The Christian Science Monitor*, 20 marzo 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/What-it-ll-take-to-forge-peace-in-cyberspace

Paul Meyer, "Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda", in *The RUSI Journal*, vol. 157, n. 1 (febbraio 2012), p. 14-19

Paul Meyer, "Norms of Responsible State Behaviour in Cyberspace", in Markus Christen, Bert Gordijn e Michele Loi (a cura di), *The Ethics of Cybersecurity*, Cham, Springer, 2020, p. 247-360, https://doi.org/10.1007/978-3-030-29053-5_18

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Ministry of Foreign Affairs of Japan, *First Meeting of G7 "Ise-Shima Cyber Group (ISCG)"*, 14 ottobre 2016, https://www.mofa.go.jp/fp/nsp/press3e_000073.html

National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*, 24 ottobre 2017, https://www.nao.org.uk/?p=67469

NATO Cooperative Cyber Defence Centre of Excellence, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, 21 luglio 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit

Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", in *International Security*, vol. 41, n. 4 (2016/17), p. 44-71, https://doi.org/10.1162/ISEC_a_00266

Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, Cambridge, Belfer Center for Science and International Affairs, 2014, https://www.belfercenter.org/node/78998

Osce, *Permanent Council Decision No. 1202*, 10 marzo 2016, https://www.osce.org/pc/227281

Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in Anna-Maria Osula e Henry Rõigas (a cura di), *International Cyber Norms: Legal Policy and Industry Perspectives*, Tallinn, NATO CCD COE Publications, 2016, p. 129-153 (capitolo 7), https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives

Presidenza del Consiglio dei ministri, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, marzo 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

Gregory J. Rattray, "An Environmental Approach to Understanding Cyberspace", in Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz (a cura di), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 253-274, https://ndupress.ndu.edu/Media/News/Article/1216674

Eva-Nour Repussard, "There Is No Attribution Problem, Only a Diplomatic One", in *E-International Relations*, 22 marzo 2020, https://www.e-ir.info/?p=82357

Christian Ruhl et al., "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads", in *Carnegie Working Papers*, febbraio 2020, https://carnegieendowment.org/publications/81110

ISSN 2610-9603 | ISBN 978-88-9368-187-2

Michael N. Schmitt e Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", in *Just Security*, 30 giugno 2017, https://www.justsecurity.org/42768

Michael N. Schmitt e Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", in *Fletcher Security Review*, vol. 1, n. 2 (2014), p. 55-73, https://059927f5-49c6-47fa-92e9-3d499a0e6da2.filesusr.com/ugd/c28a64_2610a29ebee34169988ab7a3d7c7412e.pdf

Jens Stoltenberg, "NATO Will Defend Itself", in *Prospect*, ottobre 2019, p. 4, https://www.nato.int/cps/en/natohq/news_168435.htm

UN General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/53/70), 4 dicembre 1998, http://undocs.org/A/RES/53/70

UN General Assembly, "Draft Guidelines for Appropriate Types of Confidence-Building Measures and for the Implementation of Such Measures on a global or Regional Level", Annex II in *Report of the Disarmament Commission* (A/41/42), 23 giugno 1986, https://undocs.org/A/41/42(supp)

UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201), 30 luglio 2010, http://undocs.org/A/65/201

UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98), 24 giugno 2013, http://undocs.org/A/68/98

UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), 22 luglio 2015, http://undocs.org/A/70/174

UN General Assembly, *Resolution adopted by the General Assembly on 5 December 2018* (A/RES/73/27), 11 dicembre 2018, https://undocs.org/A/RES/73/27

World Economic Forum, *The Global Risks Report 2021*, gennaio 2021, https://www.weforum.org/reports/the-global-risks-report-2021

Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", in *Wired*, 3 marzo 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", in *Wired*, 3 novembre 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet

ISSN 2610-9603 | ISBN 978-88-9368-187-2

ISSN 2610-9603 | ISBN 978-88-9368-187-2

IAI PAPERS 21 | 13 - MARZO 2021

Istituto Affari Internazionali (IAI)

L'Istituto Affari Internazionali (IAI) è un think tank indipendente, privato e non-profit, fondato nel 1965 su iniziativa di Altiero Spinelli. Lo IAI mira a promuovere la conoscenza della politica internazionale e a contribuire all'avanzamento dell'integrazione europea e della cooperazione multilaterale. Si occupa di temi internazionali di rilevanza strategica quali: integrazione europea, sicurezza e difesa, economia internazionale e governance globale, energia e clima, politica estera italiana; e delle dinamiche di cooperazione e conflitto nelle principali aree geopolitiche come Mediterraneo e Medioriente, Asia, Eurasia, Africa e Americhe. Lo IAI pubblica una rivista trimestrale in lingua inglese (*The International Spectator*), una online in italiano (*Affarinternazionali*), tre collane di libri (*Global Politics and Security*, *Quaderni IAI* e *IAI Research Studies*) e varie collane di paper legati ai progetti di ricerca (*Documenti IAI*, *IAI Papers*, ecc.).

Via dei Montecatini, 17 - I-00186 Rome, Italy
T +39 06 6976831
iai@iai.it
www.iai.it

Ultimi IAI PAPERS

Direttore: Riccardo Alcaro (r.alcaro@iai.it)

21 | 13 Luigi Martino, *Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza*

21 | 12 Nathalie Tocci et al., *From Tectonic Shifts to Winds of Change in North Africa and the Middle East: Europe's Role*

21 | 11 Carolina Polito, *La governance globale dei dati e la sovranità digitale europea*

21 | 10 Bernardo Venturi and Luca Barana, *Lake Chad: Another Protracted Crisis in the Sahel or a Regional Exception?*

21 | 09 Bruce Byiers and Luckystar Miyandazi, *Balancing Power and Consensus: Opportunities and Challenges for Increased African Integration*

21 | 08 Tsion Tadesse Abebe and Ottilia Anna Maunganidze, *Implications of COVID-19 on East Africa–EU Partnership on Migration and Forced Displacement*

21 | 07 Nicoletta Pirozzi, Luca Argenta and Paweł Tokarski, *The EU One Year after the Covid-19 Outbreak: An Italian-German Perspective*

21 | 06 Adel Abdel Ghafar, *Between Geopolitics and Geoeconomics: The Growing Role of Gulf States in the Eastern Mediterranean*

21 | 05 Alessandro Marrone and Ester Sabatino, *Cyber Defence in NATO Countries: Comparing Models*

21 | 04 Katarzyna Kubiak, *Reviewing NATO's Non-proliferation and Disarmament Policy*