Domenico Fracchiolla

La cyber-diplomacy, la nuova frontiera delle relazioni internazionali

CYBER-DIPLOMACY, THE NEW FRONTIER OF INTERNATIONAL RELATIONS

Cyber-diplomacy is conceived as the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace. As French Prime minister Clemenceau once argued that war was too serious to leave to soldiers, by the same token, cyberspace is too serious to leave to technicians. For that reason, cyber-diplomacy is the new frontier of International Relations arising from the need to politicize and internationalize the cyberspace. In the last decade, starting from the Us Strategy for Cyberspace governments are starting to develop cyber diplomatic strategies for defining and protecting their national interest in the cyberspace, appointing cyber ambassadors at international fora. However, still in 2013, only few nations had cyber diplomats and were able to speak with one voice in international negotiations, according to the Eu external cyber coordinator. The Ir literature on the subject is even more at its early stage of development. Since its first introduction, cyber-diplomacy as a term needed fundamental conceptual clarification to avoid confusion and overlapping meaning with e-diplomacy, digital diplomacy and cybersecurity. In the last years, while a number of studies defined the term cyber-diplomacy associating it to diplomatic activities, there are still fundamental points to be clarified and analysed. The aim of this paper is to present a systematic literature review to exemplify the fundamental variables of the accepted definition of cyber-diplomacy, investigated by the scientific community. Moreover, to discuss the results, to complete the conceptualization of the main lines of development of cyber-diplomacy and to underline the aspects of cyber-diplomacy on which the international community is focusing, other relevant documents will be analysed, like the reports of international research centers and the main official strategies on cyber-diplomacy adopted by national governments and international institutions (Eu, Japan, Australia). The most accredited definition of cyber-diplomacy, considering the citations and the different applications, is elaborated by Barrinha and Renard and it will be used as a reference benchmark for the operationalization of the concept. The main issues considered are cybersecurity, cybercrime, confidence-building, Internet freedom and Internet governance.

KEYWORDS *Cyber-diplomacy, Cybersecurity, Confidence Building, Cyber Norms, Internet Governance.*

Domenico Fracchiolla, University of Salerno – via G. Paolo II – 84084 Fisciano, email: dfracchiolla@unisa.it, orcid: 0000-0001-8011-1314.

ISSN 2785-0072

1. Introduzione

La *cyber-diplomacy* si presenta come la rinnovata rivendicazione del primato della politica sulla tecnica e una nuova frontiera delle relazioni internazionali, che nasce dalla necessità di politicizzare e internazionalizzare il cyberspazio. Parafrasando l'adagio del Primo ministro francese Clemenceau, così come la guerra è una materia troppo seria per essere lasciata ai soldati, il cyberspazio è materia troppo strategica per essere lasciata ad ingegneri ed informatici. La *cyber-diplomacy* si afferma come potente strumento di *soft power* contro lo *sharp power* di attori spregiudicati e si propone di colmare il vuoto di governance internazionale, sviluppando la cooperazione e l'interoperabilità nel cyberspazio, al netto di rilevanti esperienze regionali (come l'azione regolativa dell'Ue dell'ultimo lustro). Con l'accresciuta rilevanza nell'agenda politica internazionale, i primi studi *policy-oriented* sulla *cyber-diplomacy* esprimono l'interesse crescente per l'elevata interconnettività nel cyberspazio, che necessita di una dimensione internazionale della *cybersecurity*. Invece che soffermarsi solo sulla *cyber-defence* o sulla *cyberwar*, diviene fondamentale occuparsi anche di *cyber-diplomacy* (Gady e Austin 2010). Mentre alcuni studi hanno associato la *cyber-diplomacy* alle attività diplomatiche, ci sono ancora punti fondamentali riguardanti la concettualizzazione, gli ambiti e le prospettive di sviluppo da chiarire e analizzare (Barrinha e Renard 2017; Renaud e De Paoli 2020). In via preliminare, la *cyber-diplomacy* richiede una chiarificazione concettuale per evitare confusione con concetti vicini ma estranei alla nozione e alla relativa prassi, come la digital diplomacy, la *e-diplomacy* o la *digital foreign policy*, ed evitare di incorrere negli esiziali errori metodologici di ambiguità, vaghezza e del *conceptual stretching* (Sartori 1970). Inoltre, la definizione piuttosto generica e non sempre convenzionalmente condivisa dei concetti di *cyberwar* e *cyber-defence* rappresenta un altro problema di ambiguità e vaghezza nella delimitazione dei confini concettuali della *cyber-diplomacy*.

Da questa riflessione è scaturita l'esigenza di individuare le caratteristiche principali della *cyber-diplomacy* e analizzare le principali linee di ricerca che si sono sviluppate sull'argomento. Per giungere a questo obiettivo, il lavoro sviluppa un'estesa revisione della letteratura scientifica e di documenti di policy come strategie, direttive e report. La definizione più accreditata, considerate le citazioni e le diverse applicazioni, è elaborata da Barrinha e Renard (2017) e sarà utilizzata come benchmark di riferimento per la operazionalizzazione del concetto di *cyber-diplomacy*. I due autori definiscono la *cyber-diplomacy* come «l'utilizzo di risorse e funzioni diplomatiche per salvaguardare l'interesse nazionale nel cyberspazio», estendendo le funzioni proprie della dimensione esterna della sovranità e ponendo il fuoco sull'utilizzo delle risorse (strumenti

e mentalità) e delle pratiche diplomatiche per risolvere le questioni emerse nel cyberspazio. Le principali questioni considerate sono la *cybersecurity*, il cybercrime, la *confidence-building*, l'Internet freedom e l'Internet governance (Barrinha e Renard 2017).

2. L'evoluzione della cyber-diplomacy nella prassi e nei documenti ufficiali

Nel volgere di pochi anni, l'evoluzione geopolitica della presenza dello stato nel cyberspazio ha determinato gli ambiti di libertà e di competizione per il suo controllo da parte di attori privati e statali. Il cyberspazio si è trasformato, dopo la fine della guerra fredda, da dominio di policy con un moderato coinvolgimento degli stati nella fissazione degli standard delle infrastrutture cibernetiche, poco regolato, piuttosto informale, orientato e gestito da tecnici (ingegneri delle reti ed informatici) ad arena di competizione strategica dei principali attori statali della comunità internazionale (Oever 2022). Messe da parte le ambizioni di un riconoscimento generale come global common (Deibert *et al*. 2012; Mueller 2020), il moltiplicarsi delle crisi e l'emergere delle fragilità del cyberspazio (di cui le rivelazioni di Snowden sono un esempio rilevante, ma non isolato) hanno determinato una nuova fase della presenza dello stato nei processi di Internet Governance, recuperando una posizione di centralità (Oever 2022). Il cyberspazio si caratterizza, oggi, per una maggiore anarchia rispetto agli ambiti tradizionali della Comunità internazionale, ampi spazi di contestazione e rivendicazioni reciproche, forti richiami alla sovranità statale e le prospettive di un rinnovato costituzionalismo digitale (Santaniello 2021). Queste ultime, ispirate alla cooperazione internazionale, hanno prodotto norme non vincolanti e accordi ad hoc e di respiro regionale, senza riuscire ad evitare un pericoloso vuoto di governance (cfr. Lessig 2009).

La progressiva politicizzazione del cyberspazio evidenzia la crescente importanza che la *cyber-diplomacy* ha sviluppato nella prassi. Christopher Painter, antesignano della *cyber-diplomacy*, coordinatore della prima struttura diplomatica costituita in questo ambito («the Office on cyber issue») negli Stati Uniti nel 2011, sottolinea l'importanza di un serio *engagement* nella *cyber-diplomacy*, per diversi motivi. In primo luogo, per affrontare le gravi minacce che provengono dal cyberspazio, dagli attacchi cibernetici alle infrastrutture critiche al furto di dati, dal *cyber crime* al *cyber* spionaggio. Inoltre, lancia un monito per le ingerenze nei processi elettorali e le conseguenze di gravi crisi, come le note Wanna Cry, Solarwind e Microsoft, per fare esempi recenti. Infine, Painter aggiunge quali fondamentali attribuzioni, la negoziazione di accor-

di internazionali per regolamentare il cyberspazio, la promozione di alleanze tra like minded states, la funzione di de-escalation rispetto alle crisi, soprattutto ricorrendo alle *confidence capability measures*, la promozione dell'accountability internazionale (Painter 2021). Pertanto, in una prima approssimazione, allargando il campo all'azione fondamentale della società civile e delle multinazionali, le Big tech in primo luogo, la *cyber-diplomacy* può definirsi come la proiezione dell'azione diplomatica di attori statali e privati nel cyberspazio, finalizzata alla salvaguardia dei loro interessi. Per gli stati, l'interesse nazionale è cristallizzato nelle strategie nazionali di *cybersecurity* e sviluppato dalla *cyber-diplomacy* attraverso un'articolata agenda di azioni. Tra queste, figurano: l'elaborazione di *cybersecurity* policy; le strategie di *engagement*, fino alla definizione di relazioni sempre più determinanti con attori non statali; la prevenzione della pericolosa corsa agli armamenti *cyber*; l'elaborazione e adozione di norme globali cibernetiche; la definizione di un nuovo ruolo per la diplomazia. A riguardo, centrale è la riflessione sulla riorganizzazione dei dipartimenti e dei ministeri degli esteri in funzione della crescente rilevanza della *cybersecurity* e delle nuove tecnologie.

Storicamente, infatti, le prime negoziazioni sulla governance del cyberspazio sono ispirate ad un approccio *multi-stakeholder*, inteso come modello di governance che coinvolge sia i soggetti pubblici sia i soggetti privati, e al concetto di responsabilità condivisa tra la società civile, le industrie e il governo statale. Il World summit on information society (Wsis) del 2003, organizzato dalle Nazioni unite e supportato dalla partecipazione di 175 delegazioni nazionali, è il primo passaggio in questa direzione, nel tentativo di stabilire un modello di governance transnazionale e sostenibile, ispirato all'inclusività per superare le diverse frammentazioni. Questo summit è stato definito «un passo nel nuovo territorio della diplomazia globale per il ventunesimo secolo» (Kleinwachter 2004, 2). La Risoluzione dell'Assemblea generale dell'Onu (56/183) incoraggiava infatti «organizzazioni intergovernative [...] organizzazioni non governative, società civile e settore privato a contribuire e partecipare attivamente nel processo preparatorio intergovernativo e nel Summit stesso» (Un 2001, 2).

In questa fase la *cyber-diplomacy* emerge non tanto come attività intrapresa da un ristretto gruppo di uomini ma dall'azione di imprese multinazionali, attori subnazionali, reti di advocacy e individui influenti (Jönsson e Langhorne 2004). Ad esempio, la *cyber-diplomacy* è decisiva per mediare la complessità del cyberspazio, che rende difficile trovare soluzione ad alcuni problemi fondamentali, come l'attribuzione degli attacchi, risultando problematico per gli stati ricorrere alla deterrenza per rappresaglia (Barrinha e Renard 2017).

L'escalation e la gravità dell'attacco cibernetico in Estonia nel 2007 evidenziano la dimensione strategica e militare del cyberspazio, al punto da spingere molti governi a definire la dimensione interna della difesa nazionale del cyberspazio attraverso l'adozione di strategie nazionali di *cybersecurity*. In questa seconda fase, i governi nazionali elaborano strategie di *cybersecurity*, anche prevedendo risposte militari, e promuovendo il dialogo con altri membri della comunità internazionale, escludendo altri attori non-statali dai processi decisionali. Da quel momento, la *cyber-diplomacy* diventa una componente importante della politica estera dei singoli paesi, fino a quel momento riservata esclusivamente alla *cyber-defence* e alla *cyberwar* (Gady e Austin 2010). Si registra un cambiamento progressivo verso un modello di *cyber-diplomacy* ispirato al concetto di sovranità statale, in cui il cyberspazio e le infrastrutture sono sempre più percepiti come asset strategici. La *cyber-diplomacy* rende possibili forme di negoziazione tra stati rispetto a forme di *multi-stakeholder* governance. In questa fase, i singoli stati si sono focalizzati sugli aspetti strettamente domestici della *cybersecurity*, a scapito di quelli di rilievo internazionale. La dimensione internazionale delle questioni cibernetiche è affrontata solo marginalmente, per sottolineare la necessità di lavorare con partner internazionali, senza specificare molto altro. Esempi in tal senso sono la cyberspace policy review degli Stati Uniti (2009), la *cybersecurity* strategy della Gran Bretagna (2009) e il White paper on the Internet in China (2010).

Una evoluzione verso la difesa della dimensione esterna dei rapporti nel cyberspazio si realizza a partire dal 2011, con l'adozione della Us International strategy for cyberspace, il primo documento governativo interamente dedicato al cyberspazio, alla *cyber-diplomacy* e ai suoi pilastri fondamentali, quali diplomacy, defence and development (3Ds). Seguendo l'esempio dell'Ufficio per il coordinamento per il cyberspazio degli Stati Uniti, 25 Stati hanno iniziato a dotarsi di appositi uffici diplomatici, focalizzando l'attenzione sulla dimensione esterna della nuova area di politica estera. L'interesse emerso nelle diverse comunità statali però, non ha finora dato seguito a una prioritizzazione di questo dominio, che risulta essere ancora in via di sviluppo. Sul piano multilaterale, le Nazioni unite hanno mostrato un crescente interesse per la regolamentazione, in particolare per la sicurezza informatica, e le opportunità di impegno diplomatico (dimensione esterna). Nel 2004 si costituisce il primo Gruppo di esperti governativi (Gge) sulla *cybersecurity* provenienti da 15 stati (poi aumentati a 25), con il compito di esplorare le minacce nell'uso della tecnologia informatica, nonché di esaminare le misure collettive che avrebbero potuto essere messe in campo per contrastarle. Dal nulla di fatto del primo meeting del 2004, ai lenti progressi del 2010, 2013 e 2015, quando il Gge riesce ad articolare una serie di norme volontarie che promuovono il comportamento

responsabile degli stati nello spazio cibernetico e accertare che il diritto internazionale è applicabile al cyberspazio, fino alla costituzione di un nuovo Gge nel 2019, si registrano importanti passi in avanti. In particolare, dopo le critiche della Russia sul formato del Gge, per sua adesione esclusiva, che ostacola il processo democratico e marginalizza la visione dei paesi in via di sviluppo, e la forte contrapposizione dei paesi occidentali, che accusano la Russia di strumentalizzazioni intollerabili nel linguaggio ed in difesa di progetti inaccettabili per l'indebito riferimento alla sovranità statale, l'Ag Onu nel 2018 adotta sia la proposta Russa di creazione dell'Oewg, un gruppo di lavoro aperto a tutti i 193 membri delle Nazioni Unite, sia la proposta occidentale dei paesi *like-minded* di creare un nuovo Gge. Ovviamente, il lato negativo di questi risultati è rappresentato dalla moltiplicazione ed istituzionalizzazione di questi incontri, che unitamente all'ampliamento e all'approfondimento dell'agenda cibernetica, portano inesorabilmente a più «lotte politicizzate» (Deibert, 2015).

Anche la prassi nella Nato sottolinea l'importanza della cyber-diplomacy per perseguire la sicurezza nell'ambito della dimensione esterna del cyberspazio. Fin dall'attacco *cyber* in Estonia del 2007, la Nato adotta una *cyber-defence* policy (2008), il primo passo verso la securitizzazione del cyberspazio, grazie ad una significativa azione di *cyber-diplomacy*. Durante il vertice di Galles (2014) per la prima volta è prevista la possibilità di invocare la clausola di difesa collettiva dell'articolo 5 anche per gli attacchi cibernetici, pur con una valutazione da effettuarsi caso per caso. Al summit di Varsavia (2016) il cyberspazio diventa dominio operativo, al pari di quello terrestre, marittimo o aereo, e viene firmato il *cyber-defence* pledge che impegna i membri ad incrementare le capacità di difesa delle infrastrutture e reti nazionali, nonché migliorare la resilienza verso gli attacchi cibernetici.

Passando all'Ue, il percorso intrapreso nel 2015 eleva la *cyber-diplomacy* a variabile esplicativa dell'azione della governance Ue del cyberspazio. L'Ue si distingue nell'attività di regolamentazione del cyberspazio e diventa riferimento globale per altre esperienze regionali. La *Eu global strategy* (2015) rappresenta un momento importante per il primo esplicito e formale riferimento alla *cyber-diplomacy* in un documento ufficiale. L'Ue, in collaborazione con partner internazionali, si impegna nella protezione degli asset critici e dei valori nel mondo digitale, definendo gli obiettivi perseguiti, a partire dal suo ruolo *forward-looking*. L'impegno mira alla promozione di una concezione globale di Internet affinché sia reso più sicuro e libero. Tra i principali obiettivi si segnalano, in particolare: la promozione di accordi sulla responsabilità degli stati nel cyberspazio sulla base dell'applicazione del diritto internazionale; la governance digitale multilaterale; la cooperazione per un framework comune sulla *cybersecurity*. Un documento successivo, le Conclusioni del consiglio eu-

ropeo in materia di *cyber-diplomacy* (2015), incentrato sulla promozione degli interessi strategici europei e di una politica condivisa, conferma queste scelte e amplia la prospettiva. L'Ue adotta una serie di misure aggiuntive racchiuse nel Framework sulle *Joint Eu diplomatic response to malicious cyber activities* (2017), di natura preventiva, cooperativa, stabilizzatrice e restrittiva (Sebe 2022), volte a garantire, tra l'altro, supporto nel caso in cui uno degli stati europei fosse vittima di un attacco cibernetico (Art. 42 Teu, Art. 222 Tfeu). Allo stesso modo, la Eu *cyber capacity building* strategy (2018) formalizza l'intenzione dell'Unione di supportare i singoli stati nello sviluppo delle loro *cyber capabilities*, al fine di favorire l'inclusione e rafforzare la governance europea. La *cyber-diplomacy* diventa lo strumento di elezione per avanzare il modello di sovranità digitale europea, in cui la sovranità è un mezzo per garantire la protezione dei diritti e dei valori democratici fondamentali europei e non uno strumento di controllo sui cittadini.

Il richiamo ai principi liberali e democratici dello stato di diritto, nella tradizione del costituzionalismo digitale, rafforzato da un'attenta analisi del loro riconoscimento sostanziale e della loro implementazione, pone limiti al sovranismo come giustificazione degli eccessi della presenza dello stato nella governance del cyberspazio, auspicato da molti regimi autoritari. La possibile strumentalizzazione di suddetti principi, al fine di assicurare la credibilità internazionale ed evitare ricadute negative allo sviluppo della propria economia digitale, può essere sanzionata da un'analisi attenta dell'intervento dello stato nel cyberspazio, come nel caso dell'adozione da parte della Cina di un modello nazionale di protezione dei dati che emula in molti aspetti il Gdpr dell'Ue, soprattutto nei profili della protezione del consumatore, ma che non riconosce la tutela del principio della privacy come un valore fondamentale (Creemers 2022).

Anche l'Organizzazione per la sicurezza e la cooperazione in Europa (Osce) nel 2019 contribuisce alla definizione e allo sviluppo della *cyber-diplomacy*, adottando una serie di raccomandazioni volte a prevenire l'escalation di tensioni tra gli stati, in cui è individuata e scelta una strategia coordinata di *cyber-diplomacy*, sviluppando una serie di Cbms volte a fronteggiare le possibili percezioni errate da parte di uno stato sull'uso delle Ict da parte di altri stati.

In conclusione di questa fase, si segnalano tre affermazioni significative della *cyber-diplomacy* sul piano globale con relativa evoluzione della governance del cyberspazio: l'accordo Usa-Cina del 2015, per il significato e l'importanza dei firmatari, l'iniziativa Paris call della Francia del 2018, per rilanciare la centralità del modello europeo ed il compromesso raggiunto in sede Onu con i final Report del 2021 del Gge e dell'Oewg. L'esigenza di sviluppare una maggiore cooperazione e migliori relazioni internazionali nel cyberspazio porta nel 2015 all'accordo Usa-Cina sotto le Presidenze di Obama e di Xi Jinping,

che rappresenta un formale riconoscimento del ruolo della *cyber-diplomacy*, anche se sul piano bilaterale, nella gestione dei rapporti internazionali pacifici nel cyberspazio. L'obiettivo perseguito dall'accordo è di ridurre le attività di *cyber* spionaggio cinese in Usa e di ricalibrare le *cyber policy* da parte di Pechino. Nello stesso periodo, anche gli attori non statali, a partire dalle Big tech, si impegnano in azioni in questo settore: Microsoft presenta la sua Global security strategy e il suo Diplomacy team e Huawei insieme a Microsoft e Eastwest Institute sviluppano standard per influenzare gli approvvigionamenti di Ict.

L'iniziativa della Francia della *Paris call for cyber peace* (2018) propone un modello di governance basato sulla cooperazione e rilancia la dimensione esterna della *cyber-diplomacy* su base multilaterale e *multi-stakeholder*. Questo modello è diverso sia da quello *private-self-regulation* californiano, dove comunque il potere statale svolge un ruolo non secondario, e sia da quello evolutivo e assertivo della Cina, maturato negli ultimi anni, in cui emerge la competizione tra agenzie statali e gruppi di potere industriali privati come Huawei and Alibaba, portatori di proprie agende a livello nazionale ed internazionale, con linee di tendenza verso la sovranità statale in opposizione all'agenda statunitense del *cyber freedom* (Shen 2016).

Il documento del Paris Call si basa su nove principi comuni al fine di proteggere il cyberspazio ed invita tutti gli attori a lavorare insieme e incoraggiare gli Stati a cooperare con i partner del settore privato, il mondo della ricerca e la società civile. I sostenitori del Paris call si impegnano ad adottare comportamenti responsabili e attuare nel cyberspazio i principi fondamentali che si applicano nel mondo fisico. Fino ad oggi, il Paris call ha attirato oltre 1.200 sostenitori, tra cui oltre 75 governi nazionali, dimostrando un crescente riconoscimento da parte della comunità internazionale della necessità di lavorare insieme, con un approccio *multi-stakeholder*, per proteggere il cyberspazio.

Infine, anche in ambito Onu si registrano progressi con una pluralità di iniziative di *cyber-diplomacy*. L'Oewg adotta una relazione finale nel marzo 2021 che riconosce e sostiene i precedenti punti di consenso raggiunti nell' ambito Gge, avallati da tutta la comunità internazionale, al fine di promuovere la responsabilità collettiva nello spazio cibernetico. Tra le questioni nuove, Oewg sottolinea gli espliciti riferimenti alla protezione delle infrastrutture mediche e di altre specifiche infrastrutture critiche, i danni causati dalle interferenze elettorali, e, sotto insistenza della Cina, sottolinea l'importanza della Coordinated vulnerability disclosure – un meccanismo di cooperazione per la divulgazione «coordinata» e «responsabile» delle vulnerabilità tecnologiche – e della protezione della catena del valore per i prodotti Ict. Nel documento finale viene menzionata inoltre, sotto proposta coordinata di Francia e Egitto, la possibilità di istituire un Programma di azione, per far avanzare il comportamento

responsabile degli Stati, ponendo fine alle discussioni a doppio binario (Gge/Oewg) e instituendo un forum Onu permanente.

Nonostante gli sforzi collettivi e individuali, l'ultimo triennio registra un netto peggioramento delle relazioni diplomatiche *cyber*, con forti tensioni a livello multilaterale e lo stallo o l'interruzione della cooperazione internazionale a causa della guerra in Ucraina e la crisi pandemica, così come le prospettive di applicabilità del diritto internazionale al cyberspazio, in particolare in materia di self defense, diritto internazionale umanitario e l'utilizzo di contromisure nel cyberspazio. Le crescenti tensioni tra le principali potenze della comunità internazionale trasferiscono nella dimensione cibernetica le contrapposizioni della politica internazionale tradizionale, traducendo anche in questo campo gli allineamenti e le contrapposizioni basate sul combinato disposto degli alternativi sistemi di valore e della tutela degli interessi nazionali, alla base di scelte strategiche di tipo geopolitico-normativo. Oltre alle note vicende della guerra in Ucraina che contrappongono gli Stati Uniti e l'Ue alla Russia anche nella dimensione della *cyber security* come risposta agli attacchi cibernetici russi, ad inizio novembre 2022 si è tenuto il secondo vertice della Counter Ransomware initiative a Washington, raggruppando 36 paesi (tutte democrazie con l'eccezione degli Emirati Arabi Uniti) e 13 aziende al fine intraprendere azioni comuni di *cyber-diplomacy* per proteggere i propri cittadini e le proprie imprese dai crimini informatici. Aumentati del 200% nei soli Stati Uniti nell'ultimo anno, questi crimini evidenziano un forte legame con la Russia a cui è attribuito il 75% degli illeciti. Anche nel versante indo-pacifico, sempre più importante nell'attuale fase delle relazioni internazionali, la *cyber-diplomacy* è fondamentale nelle iniziative di cooperazione tra i paesi del Quadrilateral security dialogue, Quad, con progetti specifici di cooperazione *multi-stakeholder* in materia di *cyber security* e la creazione di linee di comunicazione e cooperazione diretta attraverso di Certs nazionali e i ministeri, come deciso al meeting dei *Senior cyber group* nel maggio 2022. L'adozione della strategia di sicurezza del Canada a fine novembre 2022 completa il quadro, ponendo la *cyber-diplomacy* al centro di ingenti investimenti nella regione (insieme al pattugliamento navale), per controbilanciare la politica di potenza della Cina, considerata una potenza globale disruptive, con cui il Canada dal 2018 ha rapporti tesi.

La diversità ideologica unita al fenomeno dello «SplInternet», ovvero la «balcanizzazione» di Internet provocata dalla battaglia asimmetrica tra le stesse potenze per la supremazia tecnologica a livello mondiale, rischiano di provocare e di costruire barriere digitali al libero scambio di informazioni. Lo SplInternet evidenzia (Manantan 2021) il rischio di una maggiore frammentazione e divisione tra la versione Occidentale e Orientale del cyberspazio. Il tecno-autoritarianismo diventa un nuovo formidabile rivale del cyberspazio,

in cui i dittatori difendono i loro confini virtuali e raggiungono le società dei loro rivali per intimidire l'opposizione e indebolire le istituzioni democratiche.

3. Le principali caratteristiche della cyber-diplomacy

Il termine *cyber-diplomacy* è utilizzato per la prima volta da Potter nel 2002, per descrivere l'impatto che Internet e le nuove tecnologie producono sulla diplomazia. Nella stessa direzione, la *cyber-diplomacy* è chiamata in causa per descrivere l'evoluzione della Diplomazia pubblica nell'era digitale, riferendosi all'utilizzo di strumenti e tecniche digitali per realizzare gli obiettivi diplomatici (Kleiner 2008). In entrambi i casi, si dovrebbe parlare di digital diplomacy piuttosto che di *cyber-diplomacy*: questa imprecisione terminologica è diffusa ed è continuata nel corso degli anni con sovrapposizioni seguite con l'ampliarsi degli ambiti di applicazione della digital diplomacy. Le descrizioni recenti, anche da parte di autorevoli centri di ricerca come DiploFoundation (2015, 2022), sono utilizzate in documenti ufficiali come le Conclusioni del Consiglio Ue sulla digital diplomacy il 18 luglio 2022, ed estendono il concetto della digital diplomacy fino a comprendere:

- cambiamenti prodotti da Internet negli ambiti di intervento della diplomazia (geopolitico, interdipendenza, sovranità);
- nuove issue nell' agenda diplomatica (Internet governance, *cybersecurity*, privacy protection, e-commerce);
- l'uso di nuovi strumenti digitali per la diplomazia (social media, big data).

Anche il concetto di recente elaborazione della *digital foreign policy* presenta forti sovrapposizioni con la *cyber-diplomacy*: emerso come nuovo ambito che si occupa dell'impatto della digitalizzazione sulla politica estera, la *digital foreign policy* pone il focus su riforme delle procedure, degli approcci e degli spazi della diplomazia al fine di costruire una «digital home for humanity». In particolare, le aree d'intervento, sovrapponibili con la *cyber-diplomacy*, sono: la protezione e promozione dell'interesse nazionale on line, il management della interdipendenza digitale per contenere i rischi e mantenere i benefici della interdipendenza, la digitalizzazione delle tradizionali policy issue, e-commerce, medicina online (Diplo 2021). Per superare le sovrapposizioni terminologiche e concettuali, la Diplo Foundation propone di accettare l'irrazionalità del processo di policy making che porta alle sovrapposizioni descritte e considerare che le differenze sono per lo più create dalla comunità scientifica, per descrivere con diversi prefissi, la comune realtà di Internet a seconda del focus sottolineato (Kubaliija 2015).

Pur riconoscendo il carattere bidirezionale della relazione tra il cyberspazio e la diplomazia, con l'obiettivo della chiarezza concettuale e di delineare le caratteristiche principali della *cyber-diplomacy*, questa ricerca sviluppa un'indagine di tipo qualitativo per individuare le caratteristiche fondamentali della e le relative aree di interesse della *cyber-diplomacy*, attraverso l'analisi degli articoli scientifici presenti su Google Scholar e Scopus, dopo aver illustrato brevemente la prassi rilevante. Il paragrafo si articola in tre parti: nella prima è considerata la metodologia utilizzata, nella seconda si procede all'individuazione ed analisi delle principali variabili delle definizioni di cyber-diplomacy, nella terza si procede all'individuazione delle principali linee di ricerca.

Metodologia utilizzata

La metodologia seguita si articola in 3 fasi:

- Identificazione: Sono individuati 120 articoli utilizzando il motore di ricerca Google Scholar ed inserendo la parola chiave «cyber-diplomacy». I risultati sono ordinati in base alla rilevanza degli articoli, fermandosi alla ventesima pagina dei risultati, perché nelle pagine successive i finding sono esclusivamente ripetizioni e citazioni. In aggiunta è stata condotta un'ulteriore ricerca sul database Scopus con l'inserimento della stessa parola chiave producendo risultati sovrapponibili.
- Eleggibilità: i 120 risultati sono stati ridotti ulteriormente fino a raggiungere un campione di 53 articoli utilizzando 2 criteri: rilevanza dell'articolo allo scopo della ricerca, considerata in base alla presenza di una definizione o descrizione del concetto di *cyber-diplomacy*; chiarezza in merito al carattere di scientificità della rivista sul quale l'articolo è pubblicato.

Si osserva che altri 9 altri articoli dei 120 identificati sono stati esclusi dal campione individuato perché gli autori applicano la denominazione ed in parte la nozione di digital diplomacy parlando di *cyber-diplomacy*, pur presentando gli articoli in questione caratteristiche e contenuti propri della *cyber-diplomacy*. Gli autori incorrono, pertanto, negli errori metodologici di *conceptual stretching*, vaghezza o ambiguità.

- Elaborazione dei dati: i dati sono raggruppati e rappresentanti in tabelle al fine di evidenziare: le variabili rilevanti delle definizioni di *cyber-diplomacy*; i maggiori topics all'interno degli articoli.

Le principali caratteristiche della cyber-diplomacy

Partendo dalla definizione di Barrinha e Renard (2017), utilizzata come riferimento per i numerosi e sistematici richiami nella letteratura, sono individuate quattro variabili che scompongono la definizione di *cyber-diplomacy*, al fine di elaborare una definizione operativa: security, national interest, foreign policy, *technologies*. Le prime due variabili della security e del national interest operazionalizzano l'interesse nazionale nel cyberspazio, concetto generale della definizione di Barrinha con un alto livello di astrazione; d'altra parte, le variabili della foreign policy e della *technologies* indagano la porzione della definizione che si riferisce alle risorse e alle funzioni diplomatiche. Gli autori curvano la definizione, in modo da poter mettere in maggior luce un aspetto specifico di una issue rispetto ad altre, per indagare diversi aspetti della *cyber-diplomacy*. Alcuni articoli cadono nell'errore metodologico del *conceptual stretching*, della vaghezza e dell'ambiguità facendo ricadere nel concetto di digital diplomacy 3 articoli che parlano delle variabili individuate della *cyber-diplomacy* e 6 articoli che parlano delle *technologies*.

Tab. 1 *Le variabili della cyber-diplomacy*

	Security	National Interest	Foreign Policy	Technologies
Cyber-diplomacy	21	10	16	6
Digital diplomacy*	0	0	3	6

Fonte: Elaborazione dell'autore.

* Articoli che utilizzano la denominazione di Digital Diplomacy pur riferendosi alla *cyber-diplomacy*.

La variabile della security si riferisce alla funzione fondamentale e basica della politica, di rispondere alla domanda di sicurezza, estesa alla nuova dimensione del cyberspazio; comprende quindi le articolazioni della *cyber-diplomacy* che configurano l'azione e gli strumenti atti alla messa in sicurezza del cyberspazio. All'interno del campione selezionato, questa variabile è significativa, perché registra 21 occorrenze su 53 articoli. Le definizioni di questo gruppo sottolineano l'intento di governare il dominio digitale attraverso la sicurezza: Triwahyuni sostiene che «[...] la *cyber-diplomacy* si riferisce alle strategie diplomatiche utilizzate per affrontare questioni come la sicurezza che sono sollevate nel cyberspazio» (Triwahyuni 2022, 76). Per Ghosh la *cyber-diplomacy* può essere un «[...] deciso miglioramento per gestire la natura difficile ed ingannevole della sicurezza» (Ghosh 2021,119). Sulle stesse posizioni anche Kovács (2018), Cirnu (2017) e Karim (2021). Altri autori sottolineano la dimensione esterna della *cyber-diplomacy* come strategia per favorire le relazioni pacifiche

tra gli stati e sviluppare sicurezza all'interno del cyberspazio (Dumitru Bodoni 2021; Vevera 2022; Renard 2015; Lancelot; 2020; Cirnu e Vasile 2022). Timur (2017, 249) aggiunge che «[...] la *cyber-diplomacy* ha forti implicazioni internazionali che richiedono impegno e collaborazione internazionale e insieme ad adeguate capacità di difesa, sviluppo della *cyber-diplomacy* e le strategie diplomatiche progettate per delineare l'attuale ambiente di sicurezza».

Allargando lo spettro delle possibilità e l'ampiezza della definizione incentrata sulla sicurezza, la variabile national interest si riferisce alla nozione tradizionale di interesse nazionale, che comprende un insieme di topic più ampio che può essere diversamente declinato. Complessivamente, il national interest registra 10 frequenze sul numero totale degli articoli del campione ed insieme alla security, di cui può considerarsi un'estensione concettuale, rappresenta la maggioranza delle variabili rilevanti nelle definizioni di *cyber-diplomacy*. Sono incluse le configurazioni che permettono ad uno Stato di far prevalere i propri interessi nel cyberspazio attraverso l'uso delle risorse e delle funzioni proprie della diplomazia. Calderaro e Marzuki, per esempio, definiscono la *cyber-diplomacy* in collegamento alla loro elaborazione di Internet diplomacy come «[...] l'utilizzo delle risorse diplomatiche e l'espletamento di funzioni diplomatiche per tutelare gli interessi nazionali in relazione al cyberspazio» (Calderaro e Marzouki 2022, 2). Anche Pavel considera che (2021, 193) «[...] nella *cyber-diplomacy*, la diplomazia è uno strumento per risolvere i problemi e sventare le minacce nel cyberspazio così come tutelare l'interesse nazionale». Nityasari (2020, 43) sostiene che «[...] la *cyber-diplomacy* è conosciuta come l'utilizzo delle risorse diplomatiche per sostenere l'interesse nazionale nel cyberspazio». Sulle stesse posizioni anche Tatar *et al.* (2014), Jayaskara (2021), Stoica (2020) e Hendrik Zwarts *et al.* (2022).

La variabile foreign policy si riferisce alla prima parte della definizione di Barrinha, che riguarda gli strumenti e le funzioni della diplomazia, ed intende l'implementazione della *cyber-diplomacy* come uno strumento per risolvere le questioni ed i problemi che emergono nel cyberspazio. Inoltre, intende anche l'implementazione della *cyber-diplomacy* come strumento aggiuntivo ai summit internazionali, riunioni intergovernative, ecc. Gli articoli che presentano questa variabile (16) sono molto chiari sul punto: alcuni si riferiscono alla *cyber-diplomacy* come applicazione degli strumenti e misure diplomatiche tradizionali, come Kadlecová *et al.* (2020), Wang, (2015), Cull (2011). Altri introducono all'interno della definizione le «Confidence Building Measures» che hanno come obiettivo prevenire o ridurre il rischio di conflitti riducendo o eliminando le cause di mancanza di fiducia, incomprensione, errori di calcolo tra stati» (Danca 2015, 93). Bendiek (2018, 6) allarga la definizione comprendendo, le Cbms «[...] alcuni aspetti della costruzione di norme internazionali,

della protezione dati e della libertà di espressione, dell'Internet Governance e dell'azione penale secondo gli accordi internazionali per l'assistenza giudiziaria reciproca». In modo similare anche Segal (2017, 1) sostiene che «[...] la *cyber-diplomacy* è radicata nella non interferenza negli affari interni, nella partecipazione paritaria, nell'assistenza allo sviluppo e nel rafforzamento delle capacità e nel sostegno alle Nazioni Unite e ad altre istituzioni multilaterali». Un numero residuale di articoli, infine, si riferisce alla definizione come costruzione di partenariati strategici al fine di migliorare la cooperazione internazionale (Goldman 2020; Lubin, 2020; Kumar 2022).

Infine, la variabile *technologies*, che registra sei frequenze, si riferisce all'introduzione della terminologia «tramite l'uso di strumenti tecnologici» o similari nella definizione di *cyber-diplomacy* (Ia, Blockchain, ecc.). I riferimenti sono diversi e spaziano dai «Tecnolytics states», stati nei quali «[...] la nuova *cyber-diplomacy* espande, migliora e rafforza le relazioni tra le nazioni, fa avanzare la sicurezza nazionale attraverso iniziative elettroniche futuristiche (Danda 2014, 10), ai riferimenti alla *cyber policy* 3.0 con cui «[...] la *cyber-diplomacy* deve soddisfare gli obiettivi della politica informatica 3.0 migliorando l'interoperabilità tra i diversi sistemi di governance delle Itc nazionali» (Ashkenazi 2022, 93), fino alla governance dell'Ai «[...] ora saldamente ancorata nel discorso globale ed è un sottodominio della *cyber-diplomacy*» (Georgescu 2022, 13).

Principali linee di ricerca

La seconda parte dell'analisi si concentra sulle principali linee di ricerca della *cyber-diplomacy* secondo la letteratura. Sono individuate quattro macroaree di ricerca in cui gli articoli del campione orientano la loro analisi:

- *cyber strategies*,
- *definition*;
- *application*;
- *challenges*.

Anche in questo caso, come per l'individuazione delle caratteristiche fondamentali, alcuni articoli cadono negli errori metodologici di cui sopra, denominando digital diplomacy linee di ricerca proprie della *cyber-diplomacy*. In particolare, la macroarea delle *application* si presta maggiormente agli errori di ambiguità e di *conceptual stretching* perché capovolge i concetti di domanda e offerta di *cyber-diplomacy*: l'attività propria della digital diplomacy dell'utilizzo dei social media per svolgere l'attività diplomatica è erroneamente associata all'applicazione della *cyber-diplomacy* alle relazioni internazionali, come con attività di formazione e lo sviluppo di *capacity building* (4 articoli).

Segue la tabella contenente il conteggio delle linee di ricerca:

Tab. 2 *Linee di ricerca*

	Cyber Policy	Definition	Application	Challenges
Topics cyber-diplomacy	36	2	11	4
Topics Digital diplomacy *	1	1	4	2

Fonte: elaborazione dell'autore.

*Vale quanto considerato in precedenza. Dal campione originario sono esclusi 9 articoli che presentano la denominazione Digital diplomacy anche se i contenuti sono in parte o in toto rientranti nella *cyber-diplomacy*.

Il topic «cyber policy» si focalizza principalmente sulle *cyber operations* e le National security strategies da applicare per prevenire e/o mitigare i rischi nel cyberspazio. Con 36 frequenze su 53 articoli del campione rappresenta la parte maggioritaria dello sforzo di analisi della comunità scientifica fino in tema di *cyber-diplomacy*. Fondamentalmente questi articoli riconoscono la *cyber-diplomacy* come uno strumento potente a disposizione dei diversi corpi diplomatici per dirimere eventuali conflitti e/o issue all'interno del cyberspazio, focalizzandosi, in molti casi, sull'analisi e valutazione della produzione normativa. Tale azione regolativa può avvenire per mezzo di:

- summit internazionali;
- accordi bilaterali e multilaterali;
- cooperazione internazionale

Alcuni articoli non fanno chiarezza sul modo in cui la *cyber-diplomacy* dovrebbe intervenire all'interno di contesti di messa in sicurezza del cyberspazio (Es. Hurel 2022).

Si registrano alcune ricerche comparative finalizzate ad individuare correlazioni tra i contenuti delle National *cyber security* strategy adottate e le specificità di tipo economico o politico dei paesi considerati (Tatar *et al.* 2014), (Kovács 2018). Alcuni autori si concentrano sulle misure impiegate per combattere le attività criminali informatiche e sulle tipologie di strategie cibernetiche applicate (Danda 2014). Altri evidenziano l'enfasi sul bisogno di proteggere le informazioni e le infrastrutture critiche, come Hurel (2022), Georgescu (2022) e Vevera (2022). Un gruppo più ristretto di autori sottolinea l'importanza di creare partenariati internazionali, per definire la creazione di *cyber strategies* congiunte Kadlecová *et al.* (2020). Infine, alcuni studi si concentrano nella spiegazione dei nuovi strumenti di policy (Miadzvetskaya e Wessel 2022) ed un numero ristrettissimo si concentra nell'illustrare successi e/o fallimenti di policy implementate da attori statali (Jayasekara 2021). Questo particolare

campo di ricerca nasconde la possibile sovrapposizione tra la nozione di *cyber-diplomacy* e quella di *cybersecurity*. Infatti, si è potuto notare come diversi autori eguagliano il rafforzamento delle normative a favore della *cybersecurity* alla *cyber-diplomacy*, sostituendola o sovrapponendola (Tsvetkova 2020). Tuttavia, all'interno di questi articoli non è presente una vera e propria spiegazione di come la *cyber-diplomacy* debba essere applicata per raggiungere gli scopi sopra citati (Karim 2021). E ancora, la maggior parte degli autori è rimasta ancorata alla nozione e/o applicazione tradizionale di diplomazia, utilizzando logiche e strumenti non sempre adatti per il contesto digitale. È interessante rilevare che all'interno di un articolo quando è presente la variabile «security» spesso è presente anche il topic «cyber policy» (Iswardhana 2021; Dumitru e Bodoni 2021).

Il topic «application» registra 11 frequenze e si focalizza su come gli attori internazionali, posti su differenti livelli, applicano la *cyber-diplomacy* nel contesto delle relazioni internazionali. Alcune ricerche sono finalizzate ad individuare empiricamente il modo in cui è stata applicata la *cyber-diplomacy* da attori statali in determinati contesti regionali (Hadj Zargarbashi e Movahhedian 2018; Tabatabaei *et al.* 2017; Tabatabaei *et al.* 2016. Altre ricerche sono finalizzate ad individuare lo sviluppo delle *capacity building* da parte delle organizzazioni internazionali che applicano la *cyber-diplomacy* (Georgescu 2022). Infine, un certo numero di studi individua ed analizza le applicazioni tecnologiche (Triwahyuni 2022), concentrandosi anche sulla formazione dei diplomatici, soprattutto quelli dei paesi in via di sviluppo. In merito, Zwarts (2022) propone il *cyber-diplomacy* awareness framework (cyber-diplomacyfa).

Il topic «challenges» registra 4 frequenze e si focalizza sulle sfide che la *cyber-diplomacy* deve affrontare all'interno del cyberspazio, per risolvere delle criticità insite in quest'ultimo, dalla pandemia Covid-19 e le sue conseguenze, all'utilizzo degli strumenti digitali per migliorare il lavoro diplomatico (Pavel 2021), ai problemi fondamentali di attribuzione in caso di *cyber* attacco, soprattutto rispetto alle posizioni do chi nega si tratti di azioni di *cyber warfare* o di pericoli alla sicurezza nazionale (Lancelot 2020). Gli articoli non fanno riferimento ad uno specifico campo d'azione o applicazione, ma solo alle competenze che i diplomatici tradizionali devono acquisire per applicare la *cyber-diplomacy* (corsi di aggiornamento, conoscenza del digitale). Entrambi i topic delle «application» e delle «challenges», nonostante il numero più limitato di frequenze, si confrontano con un'area di ricerca di assoluto interesse e di grande prospettiva, anche se ancora agli albori.

Infine, il topic «definition» si focalizza nell'elaborazione della definizione, con una spiegazione analitica che declini la *cyber-diplomacy* in differenti modi. Si osserva immediatamente che il limitato interesse per questo ambito

di ricerca, che presenta solo 2 frequenze, non trova riscontro in una ricchezza di analisi e ricerche consolidate, salvo la definizione di Berrinha utilizzata in questo lavoro.

Mihai (2022) e Cirnu (2017) si misurano con le definizioni giungendo alle stesse conclusioni di Berrinha. Il primo si distingue per una sottolineatura dell'obiettivo del perseguimento dell'interesse nazionale, e l'altro per la soluzione dei problemi nel cyberspazio. In quest'ultimo caso, la dimensione internazionale non è solo gregaria o affiancata a quella interna dell'interesse statale, ma è esplicitamente menzionata come principale scopo.

4. Conclusioni

Nonostante la centralità della *cyber-diplomacy* nell'attuale comunità internazionale e alcune iniziative statali innovative, come la nomina di *cyber ambassador* presso la Silicon Valley, le difficoltà di trovare soluzioni condivise ai problemi internazionali posti dalla governance del cyberspazio sono evidenti. Per quanto concerne la riflessione scientifica è ancora allo stadio iniziale e non riesce a seguire il passo dell'evoluzione della prassi. Non solo le tre dimensioni fondamentali di sicurezza, difesa dell'interesse nazionale e diritti individuali non ricevono la dovuta attenzione, ma anche fondamentali questioni metodologiche e definitorie sono tralasciate dalla letteratura meno attenta che si occupa di *cyber-diplomacy*.

Tornando alla prima domanda di ricerca sulla definizione delle principali caratteristiche della *cyber-diplomacy*, la prassi evidenzia una lenta ma costante evoluzione ed affermazione nella gestione dei rapporti internazionali del cyberspazio, non solo nella dimensione interna della sicurezza e della difesa degli interessi nazionali, ma anche e soprattutto nella dimensione esterna, dove il contributo della *cyber-diplomacy* potrà essere decisivo vista la maggiore intensità del carattere di anarchia del cyberspazio. L'analisi sviluppata dimostra come la *cyber-diplomacy* sia ancora un'attività prettamente condotta dagli stati, a cui si applicano buona parte delle regole e dei framework tradizionali della diplomazia, aggiungendo significative innovazioni, considerate la peculiarità del cyberspazio per caratteristiche ed intensità dei livelli di anarchia. Gli sforzi degli stati si sono moltiplicati, affiancando gli attori privati con la crescente politicizzazione e le prospettive di una maggiore cooperazione internazionale. L'Australian institute of international affairs (2021) precisa alcuni aspetti della definizione con un approccio pragmatico, a partire dalla diffusione di pratiche di *capacity building* e di Confidence building measures (Cbms) per creare le condizioni per la formazione, produzione e adozione di *cyber norms*.

La *capacity building*, orientata alla *cybersecurity*, è sviluppata attraverso la promozione di competenze tecniche, diplomatiche e di governance necessarie per sviluppare la resilienza contro le minacce on line, la formazione di computer *incident response teams* ed il rafforzamento di corpi di forze dell'ordine. A queste, si aggiungono le Cbms, che favoriscono la condivisione delle informazioni e mitigano l'incertezza, migliorando la trasparenza e le possibilità di gestione delle crisi e di strategie di risanamento tra gli stati. Infine, anche la promozione dell'attività di codificazione delle *cyber norms*, standard di comportamento appropriato concernente l'uso delle Ict, adottate su base volontaria e non vincolante, ne beneficia, in un contesto di mantenimento della stabilità e della sicurezza internazionale. Come specificato dal Manuale di Tallin, le *cyber norms* possono essere codificate nel diritto internazionale per regolamentare i conflitti *cyber* e il *cyber warfare*, mentre il diritto internazionale rimane sempre il loro fondamento giuridico.

Nella letteratura si osserva come le caratteristiche principali della *cyber-diplomacy* presentino un forte riferimento ai caratteri tradizionali della diplomazia applicati al cyberspazio, e sono individuate nelle variabili della sicurezza, dell'interesse nazionale e della politica estera. Queste variabili articolano il *capacity building*, superando anche l'orizzonte fondamentale dell'elaborazione di *cybersecurity* policy.

Una variabile aggiuntiva è quella della tecnologia che rappresenta l'apertura verso le nuove frontiere delle implicazioni tecnologiche della definizione degli interessi statali nel cyberspazio, che spaziano dall'Ai alle block chains, alla più generale interoperabilità tra i diversi sistemi di governance Ict nazionali. Le Cbms, insieme ai ritrovati tecnologici al servizio della *cyber-diplomacy*, rispondono all'evoluzione più specifica della diplomazia nel cyberspazio, per il carattere di profonda incertezza e opacità di alcuni aspetti essenziali della nuova dimensione.

Per quanto concerne la domanda di ricerca che indaga le principali linee di ricerca della *cyber-diplomacy* secondo la letteratura, è possibile individuare lo studio e l'analisi dell'attività statale di elaborazione delle National *cybersecurity* strategy e l'attività normativa dei Fora internazionali e regionali, in particolare lo slancio regolatorio dell'Ue, come le linee di ricerca più seguite e sviluppate. Le applicazioni e le sfide rappresentano la parte più interessante, perché evidenziano gli ambiti nei quali la prassi e la comunità scientifica devono concentrarsi per dare sostanza al carattere innovativo della *cyber-diplomacy*. Infine, la scarsa attenzione dedicata dagli studiosi alle questioni definitorie riflette la difficoltà di queste analisi per la confusione presente in parte della letteratura, che ha seguito l'evoluzione, a volte incoerente, della prassi. Sarebbe opportuno combinare strumenti di ricerca come interviste, osservazioni empiriche e ana-

lisi della letteratura per esplorare il carattere innovativo della *cyber-diplomacy* come strumento di elezione delle relazioni pacifiche degli attori della Comunità Internazionale nel cyberspazio.

L'esigenza delle diplomazie nazionali di dotarsi di personale qualificato in questo ambito lascerebbe ampio spazio ad una virtuosa collaborazione tra accademia e istituzioni; il campo della Cbms e della capability building è un esempio in tale direzione, ma al momento i tentativi esperiti non hanno prodotto risultati completamente convincenti.

Riferimenti bibliografici

Ashkenazi, A. (2022), *Cyber-diplomacy 3.0 - «Agile Diplomacy» to Promote Security and Innovation*, in «International Journal of Cyber-diplomacy», 3, pp. 81-98.

Attatfa, A., Renaud, K. e De Paoli, S. (2020), *Cyber-diplomacy: A Systematic Literature Review*, in «Procedia Computer Science », 176, pp. 60-69.

Barrinha, A. e Renard, T. (2017), *Cyber-diplomacy: the Making of an International Society in the Digital Age*, in «Global Affairs», 3(4-5), pp. 353-364.

Barrinha, A., e Renard, T. (2020), *Power and Diplomacy in the Post-liberal Cyberspace*, in «International Affairs», 96(3), pp. 749-766.

Bendiek, A. (2018), *The Eu as a Force for Peace in International Cyber-diplomacy*, Stiftung Wissenschaft und Politik. Availabe at: https://nbnresolving.org/urn:nbn:de:0168-ssoar-57428-2. Consultato il 20 dicembre 2022.

Calderaro, A. e Marzouki, M. (2022), *Global Internet Governance: an Uncharted Diplomacy Terrain*, in A. Calderaro e M. Marzouki (eds), *Internet Diplomacy: Shaping the Global Politics of Cyberspace*, Lanham (Md), Rowman & Littlefield, pp. 1-18.

Chernenko, E. (2018), *Russia's Cyber-diplomacy*, in «Hacks, Leaks and Disruptions. Russian Cyber Strategies», pp. 43-49.

Cîrnu C.E. (2017), *Cyber-diplomacy — Addressing the Gap in Strategic Cyber Policy*, in «The Market for Ideas», 1, pp.7-8

Cîrnu, C.E. e Vasile, P.C. (2022), *A Blockchain-Based Application as Part of a Digital Diplomacy Approach to Facilitate and Advance Cyber-diplomacy*, in «International Journal of Cyber-diplomacy», 3, pp. 51-60

Cremers, R. (2022), *China's emerging data protection framework*, in «Journal of Cybersecurity», pp. 1-12.

Cull, N.J. (2011), *WikiLeaks, Public Diplomacy 2.0 and the State of Digital Public Diplomacy*, in «Place Branding and Public Diplomacy», 7(1), pp. 1-8.

Danca, D. (2015), *Cyber-diplomacy — A New Component of Foreign Policy*, in «Journal of Law and Administrative Sciences», 3, pp. 91-97.

Danda, S. J. (2014), *An Evaluation of Cyber-diplomacy against the Threat of Cyber Crime: The Case of the Us Prism Programme Leak, Doctoral Dissertation*, University of Zimbabwe, pp. 1-100.

Deibert, R.J. e Crete-Nishihata, M. (2012), *Global Governance and the Spread of Cyberspace Controls*, in «Global Governance», 18, pp. 339-361.

Dumitru, D. e Bodoni, C. (2021), *Extension of International Humanitarian Law Order in the Information Area through Digital Diplomacy*, in «Strategic Impact», 80(3), pp. 86-102.

Gady, F.S. e Austin, G. (2010), *Russia, the United States and Cyber-diplomacy: Opening the Doors*, in «EastWest Institute», pp. 1-19.

Georgescu, A. (2022), *Cyber-diplomacy in the Governance of Emerging Ai Technologies - A Transatlantic Example*, in «International Journal of Cyber-diplomacy», 3, pp. 13-22.

Ghosh, S. (2021), *Cyber Security and Political Aspects: India Context*, in «Indian Journals» 8(2), pp. 119-130.

Goldman, E. O. (2020), *From Reaction to Action: Adopting a Competitive Posture in Cyber-diplomacy*, in «Texas National Security Review», 3(4), pp. 1-18.

Hadj Zargarbashi, S.R. e Movahhedian, E. (2018), *Cyber-diplomacy Influence on Viewpoint of Iranian Users of Cyberspace (Case Study: USA Dar Farsi Facebook Webpage)*, in «New Media Studies», 4(15), pp. 73-112.

Hurel, L. M. (2022), *Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America*, in «Global Security Review», 2(7), pp. 21-31.

Iswardhana, M.R. (2021), *Cyber-diplomacy and Protection Measures Against Threats of Information Communication Technology in Indonesia*, in «Journal of Islamic World and Politics», 5(2), pp. 343-367.

Jayasekara, R. (2021), *China's Cyber-diplomacy under President Xi Jinpin*, in «Emerging Scholars Symposium», 1(5), pp. 37-44.

Jönsson, C. e Langhorne, R. (2004), *Diplomacy: Three Volume Set*, Thousand Oaks (Ca), Sage.

Kadlecová, L., Meyer, N., Cos, R. e Ravinet, P. (2020), *Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field*, in «Science Diplomacy in the Making: Case-based insights from the S4D4C project», pp. 62-96.

Karim, M.E. (2021), *Cybersecurity and Cyber-diplomacy at the Crossroad: An Appraisal of Evolving International Legal Developments in Bangladesh Context*, in «Dhaka University Law Journal», pp. 243-265.

Kleinwächter, W. (2004), *Wsis: A New Diplomacy? Multi-stakeholder Approach and Bottom-up Policy in Global Ict Governance*, in «Information Technology and International Development», 1(3-4), pp. 3-14.

Kovács, L. (2018), *National Cybersecurity as the Cornerstone of National Security*, in «Land Forces Academy Review», 23(2), pp. 113-120.

Kumar, R. e Aryan, A., (2022), *The Roadmap of India's Foreign Relations and Usa. Geo-Politics Interests in the New World Order*, in «International Journal of Multidisciplinary», 7(11), pp. 45-53.

Kumar, A. (2022), *Cyber-diplomacy – The Concept, Evolution and its Applicability*, in «International Journal of Cyber-diplomacy», 3, pp. 23-32.

Lancelot, J. (2020), *Cyber-diplomacy: Cyberwarfare and the Rules of Engagement*, in «Journal of Cyber Security Technology», 4(4), pp. 240-254.

Lessig, L. (2009), *Code: And Other Laws of Cyberspace*. ReadHowYouWant.com.

Lubin, A. (2020), *Cyber Insurance as Cyber-diplomacy*, in «Middle East institute», pp. 22-37.

Manantan, M. B. F. (2021), *Defining Cyber-diplomacy*, Australian Institute, 10 novembre, https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy. Consultato il 20 dicembre 2022.

Miadzvetskaya, Y. e Wessel, R.A. (2022), *The Externalisation of the Eu's Cybersecurity Regime: The Cyber-diplomacy Toolbox*, in «European Papers», 7(1), pp. 413-438.

Mueller, M. L. (2020). *Against Sovereignty in Cyberspace*, in «International Studies Review», 22(4), pp. 779-801.

Nityasari, A. (2021), *Technology Disruptions in International Relations: The Needs for Cyber-diplomacy by Indonesia*, in «Global South Review», 2(1), pp. 36-50.

Oever, N. (2011), *5G and the Notion of Network Ideology, or: The Limitation of Socioeconomic Imaginaries*, in «Telecommunications Policy», doi: 10.1016/j.telpol.2022.102442.

Osce (2016), *Decision No 1202: Osce Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, https://www.osce.org/files/f/documents/d/a/227281.pdf. Consultato il 20 dicembre 2022.

Pavel, T. (2021), *Cyber Dyplomacy and the Covid-19 - What is Cyber-diplomacy and how was it Affected by the Covid-19 Era?*, in «International Organizations and States' Response to Covid-19», 1(11), pp. 191-207.

Renard, T. (2015), *Us-China Cybersecurity Agreement: A Good Case of Cyber-diplomacy, Egmont Commentary*, https://www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy. Consultato il 20 dicembre 2022.

Santaniello, M. (2021), *From Governance Denial to State Regulation: A Controversy-Based Typology of Internet Governance Models*, in B. Haggart, N. Tusikov e J.A. Scholte (eds), «*Power and Authority in Internet Governance. Return of the State?*», Londra, Routledge, pp.15-36

Sartori, G. (1970), *Concept Misformation in Comparative Politics*, in «American political science review», 64(4), pp. 1033-1053.

Sebe, M. (2022). *On Digital Diplomacy. Key Issues, paper presentato alla International Conference on Cybersecurity and Cybercrime*, 9, 23-28. doi: 10.19107/CYBERCON.2022.02.

Segal, A. (2017), *Chinese Cyber-diplomacy in a New Era of Uncertainty*, in «Aegis Paper Series», 1703, pp. 1-23.

Sen, H. (2016), *China and Global Internet Governance: Toward an Alternative Analytical Framework*, in «Chinese Journal of Communication», 9(3), pp-304-324.

Solana, B.A. (2022), *Shifting from Kinetic to Cyber*, in «International Journal of Cyber-diplomacy», 3, pp. 3-11.

Stoica, A. (2020), *From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment*, in «International Journal of Cyber-diplomacy», 1(1), pp. 27-35.

Tabatabaei, S.M., Salimi, H. e Movahedian, E. (2016), *Us Cyber-diplomacy Influence on Viewpoint of Iranian Users of Cyberspace (Case Study: Voice of America Website)*, in «New Media Studies», 4(15), pp. 113-129

Tatar, Ü., Çalik, O., Çelik, M. e Karabacak, B. (2014), *A Comparative Analysis of the National Cybersecurity Strategies of Leading Nations*, paper presentato alla International Conference on Cyber Warfare and Security, Baltimore (Md), United States, 10 marzo.

Timur, F. G. C. (2017), *The Rise of Cyber-diplomacy Asean's Perspective in Cybersecurity*, in «KnE Social Sciences», pp. 244-250.

Tsvetkova, N. (2020), *Russian Digital Diplomacy: A Rising Cyber Soft Power?*, in «Russia's Public Diplomacy», pp. 103-117.

Triwahyuni, D. (2022), *Indonesia Digital Economic Diplomacy during the Covid-19 Global Pandemic*, in «Journal of Eastern European and Central Asian Research», 9(1), pp. 75-83.

Un General Assembly (2001), *Resolution N. 56/183. World Summit on the Information Society*, Geneve, https://222.itu.int/net/wsi/doc/background/resolutions/56-183-unga-2002-pdf. Consultato 20 luglio 2022

Vevera, A. V. (2022), *Critical Infrastructure Diplomacy–Tracing the Contours of a New Practice*, in «International Journal of Cyber-diplomacy», 3, pp. 41-49.

Wang, W. (2015), *Analysis on China's Cyber-diplomacy*. in D. Mierzejewski e K. Żakowski «*On Their Own Paths. Japan and China Responses to the Global and Regional Challenges*», Łódź, Łódź University Press.

Zwarts, H., Du Toit, J. e Von Solms, B. (2022), *A Cyber-diplomacy and Cybersecurity Awareness Framework (cyber-diplomacyaf) for Developing Countries*, paper presentato alla European Conference on Cyber Warfare and Security, Chester, United Kingdom, 16-17 giugno.