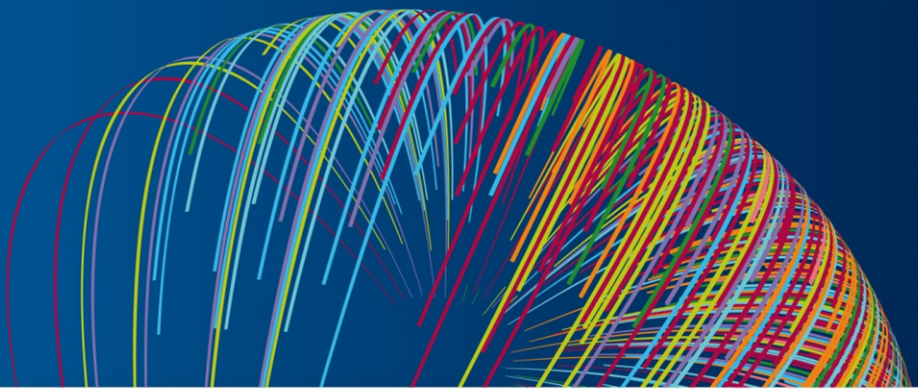
Osservatorio
di Politica internazionale



Senato
della Repubblica

Camera
dei deputati

Ministero
degli Affari Esteri
e della Cooperazione
Internazionale

LA CONDOTTA CINESE E NORDCOREANA NELLE "ZONE GRIGIE" DEL DOMINIO MARITTIMO E CIBERNETICO: PROSPETTIVE PER IL FUTURO DELLE ALLEANZE DI SICUREZZA

Luglio 2021

178

Approfondimenti

A cura dell'Istituto per gli Studi di Politica Internazionale

OSSERVATORIO DI POLITICA INTERNAZIONALE

Approfondimento ISPI

LA CONDOTTA CINESE E NORDCOREANA NELLE "ZONE GRIGIE" DEL DOMINIO MARITTIMO E CIBERNETICO: PROSPETTIVE PER IL FUTURO DELLE ALLEANZE DI SICUREZZA IN ASIA ORIENTALE

Francesca Frassineti

Francesca Frassineti, Associate Research Fellow Osservatorio Asia, ISPI

LA CONDOTTA CINESE E NORDCOREANA NELLE "ZONE GRIGIE" DEL DOMINIO MARITTIMO E CIBERNETICO: PROSPETTIVE PER IL FUTURO DELLE ALLEANZE DI SICUREZZA IN ASIA ORIENTALE

INDICE

Executive Summary

Recentemente si è registrato il ritorno nel dibattito sulla difesa dell'espressione "zona grigia" utilizzata dagli analisti e dai policy makers per riferirsi all'impiego di tattiche che sfidano lo status quo senza innescare un'escalation che sfoci in un confronto bellico esteso. Queste sfide altresì descritte nei decenni passati con termini quali guerra ibrida, conflitto a bassa intensità, guerra asimmetrica e non convenzionale, identificano scenari di interazioni conflittuali che influenzano e alterano una competizione strategica altrimenti caratterizzata da un certo grado di stabilità e prevedibilità.

La Cina è uno dei principali attori internazionali a muoversi entro la "zona grigia" e ha reso questo approccio una componente sostanziale della sua strategia politico-militare nell'Asia-Pacifico al fine di spostare l'equilibrio di potere regionale a suo favore e incidere sulla credibilità degli impegni degli Stati Uniti a sostegno della difesa degli alleati storici come il Giappone, la Corea del Sud o l'Australia. I tentativi di Pechino di raggiungere alcuni obiettivi di sicurezza senza ricorrere a un uso diretto e cospicuo della forza militare sono visibili da anni nel dominio marittimo e aereo in particolare nel Mar Cinese Meridionale e Orientale. La rilevanza delle azioni cinesi, messe in atto attraverso agenzie di *law enforcement* integrate nella catena di comando militare, valica i confini dei casi oggetto di questo studio, perché potrebbero costituire un precedente potenzialmente replicabile nel quadro di altre dispute nella regione, ma anche al di fuori di essa, e compromettere la gestione degli spazi marittimi contestati.

Dall'armistizio del luglio 1953 la Corea del Nord ha continuato con vari gradi di intensità a mettere in atto provocazioni e aggressioni militari circoscritte ai danni della Corea del Sud, ma la superiorità dell'alleanza bilaterale di sicurezza tra Washington e Seoul è riuscita a scoraggiare Pyongyang dal lanciare una nuova aggressione su larga scala. Nonostante ciò, la minaccia asimmetrica nordcoreana si è intensificata da quando le operazioni nel dominio cibernetico si sono aggiunte a un deterrente nucleare e missilistico che sotto Kim Jong Un è diventato più credibile e integrato. L'attenzione internazionale rivolta alla Corea del Nord continua a concentrarsi sul suo programma di armi di distruzione di massa, essendo questo la componente più visibile. Tuttavia, le operazioni informatiche offensive offrono al leader un'alternativa a basso costo per esercitare ulteriore pressione sulla comunità internazionale e garantire la sopravvivenza del regime della famiglia Kim in una fase in cui l'economia nordcoreana è messa in ginocchio dall'effetto congiunto delle sanzioni internazionali e dell'isolamento autoimposto per impedire la diffusione nel paese della pandemia da Covid-19.

L'approfondimento intende fare luce sull'uso deliberato e integrato di vari strumenti del potere politico, economico e militare da parte di Pechino e di Pyongyang rispettivamente nello spazio marittimo e cibernetico le cui ripercussioni, soprattutto considerate le caratteristiche del secondo dominio, trascendono i rapporti tra gli stati dell'Asia orientale. Il regime cinese e quello nordcoreano sfidano l'ambiente strategico beneficiando dell'ambiguità tipica delle tattiche coercitive della "zona grigia" relativamente alla natura dello scontro e all'incertezza del quadro legislativo e politico di riferimento che aumenta quando compaiono degli attori non statali. Pechino e Pyongyang traggono ulteriori vantaggi dalle vulnerabilità connesse alle dinamiche tra gli Stati Uniti, il Giappone e la Corea del Sud. Operando al di sotto della soglia che giustificherebbe altrimenti una risposta collettiva secondo le clausole previste dai trattati bilaterali che compongono il sistema di alleanze cosiddetto "*hub-and-spoke*", Cina e Corea del Nord portano alla luce le difficoltà di coordinamento tra Washington e i suoi alleati legate soprattutto alle percezioni difformi circa l'origine delle minacce e all'antagonismo storico tra Seoul e Tokyo che negli anni ha ostacolato qualsiasi tentativo di formalizzare un'alleanza trilaterale.

LE AZIONI CINESI NELLA "ZONA GRIGIA" DEL MAR CINESE MERIDIONALE

Dai primi anni Novanta la rinnovata enfasi sulla centralità del dominio marittimo ha reso necessario, nel contesto del più ampio sforzo di militarizzazione della Cina, un processo di modernizzazione navale in funzione degli obiettivi strategici del Partito comunista cinese (Pcc) tra cui la riunificazione nazionale, il controllo sui mari regionali fino alla prima catena di isole, il rafforzamento della posizione secondo cui Pechino abbia il diritto di regolamentare le attività militari straniere nella sua zona economica esclusiva di 200 miglia, la difesa delle linee di comunicazione marittima e commerciale della Cina, in particolare quelle che la collegano al Golfo Persico, e la marginalizzazione dell'influenza statunitense nel Pacifico occidentale. Coerentemente con questi interessi la Marina dell'Esercito popolare di liberazione (Epl) partecipa al mantenimento dell'intricata rete integrata di piattaforme di difesa aerea e missilistica A2/AD (*Anti Access/Area Denial*) concentrata intorno a Taiwan e nel Mar Cinese Meridionale, per ostacolare le operazioni di pattugliamento in tempo di pace delle forze statunitensi e il loro intervento in caso di crisi.

Nel 2013 Xi Jinping è tornato a sottolineare attraverso il concetto di "gestione strategica dei mari" il ruolo fondamentale dello spazio marittimo per lo sviluppo economico interno e la difesa degli interessi cinesi in termini di sovranità e sicurezza. L'esaltazione della difesa dei diritti marittimi nazionali da parte del leader, unitamente alle spinte nazionaliste e alle pressioni dei quadri militari, ha indotto le forze navali cinesi a esibire maggiore risolutezza nel contesto delle dispute marittime e territoriali in cui Pechino è coinvolta e su cui il Partito non è disposto a negoziare trattandosi di "sacre acque territoriali" e di isole che sono parte integrante del territorio nazionale da "tempo immemore".[1] Questa rinnovata assertività è stata parzialmente "controllata" dalla necessità di mantenere la stabilità nel dominio marittimo, in particolare per gestire le ripercussioni dell'ascesa navale cinese e mitigare il rischio che i vicini del Sudest asiatico sviluppassero relazioni diplomatiche e di cooperazione militare più assidue con gli Stati Uniti, l'India e il Giappone.[2] La ricalibratura dell'assertività cinese è emersa soprattutto dopo che Pechino ha sostanzialmente alterato lo status quo in gran parte del Mar Cinese Meridionale garantendosene l'effettivo controllo attraverso l'occupazione di isole e affioramenti, la costruzione di elementi territoriali ex novo e la loro riconversione in avamposti civili e militari. Ottenuta la trasformazione territoriale del Mar Cinese Meridionale in funzione dei propri obiettivi strategici, la Cina si è potuta dedicare al consolidamento delle sue posizioni piuttosto che a un'ulteriore espansione. Benché costruire isole non sia illegale, agire come se ciò producesse dei diritti mette in discussione il diritto marittimo; dotarle di strutture per supportare batterie missilistiche e piattaforme per caccia, bombardieri e veicoli aerei senza equipaggio, le "militarizza". Non è casuale peraltro che nel novembre 2013 Xi abbia annunciato la *Belt and Road Initiative* (Bri), allora chiamata *One Belt One Road* (Obor), il cui braccio marittimo passa per il Mar Cinese Meridionale con due delle sue rotte principali. Ufficialmente la Bri resta un progetto infrastrutturale di sviluppo economico ma il legame con l'Epl e la Marina è significativo. A questo proposito, è utile includere nel quadro anche l'inaugurazione, nel 2016, della prima base navale d'oltremare cinese a Doraleh (Gibuti) che ha dato a Pechino accesso a vie marittime al di fuori dei confini regionali e ha portato le sue navi alle porte del Mediterraneo.

---

[1] F. Lasserre, "Once Forgotten Reefs... Historical Images in the Scramble for the South China Sea", *Cybergeo: European Journal of Geography*, vol. 92, n. 4, 1999.

[2] J. Kraska e M. Monti, "The Law of Naval Warfare and China's Maritime Militia", *International Law Studies*, vol. 91, n. 1, 2015.

La Cina non ha ancora utilizzato gli avamposti artificiali nel Mar Cinese Meridionale per interferire con la libertà di navigazione, tuttavia si teme che Pechino possa sfruttarli per dispiegare gradualmente la capacità fisica di imporre dei vincoli alla libera circolazione marittima. Queste strutture sono ritenute strategicamente significative perché facilitano la proiezione della potenza aerea della Cina sullo spazio marittimo a sostegno sia delle sue capacità A2/AD sia di un futuro tentativo di imporre una zona di identificazione della difesa aerea nel Mar Cinese Meridionale. Al contempo, essendo così visibili, minimizzano uno dei problemi principali connessi alle azioni nella "zona grigia" ossia quello dell'attribuzione. Le incertezze sull'attribuzione delle attività aumentano anche quando in campo entrano attori irregolari che nel caso della Cina, come vedremo, rispondono prevalentemente al nome di "terza" forza marittima. Se nel Mar Cinese Meridionale il dilemma dell'attribuzione delle azioni nella "zona grigia" è meno sentito, resta la difficoltà di come, e se, rispondere. Gli Stati Uniti hanno aumentato la loro presenza in queste acque anche attraverso pattuglie marittime, esercitazioni militari e una maggiore assistenza alla sicurezza di alcuni stati litoranei ma nessuno di questi interventi è stato mirato e ha avuto l'effetto di frenare o annullare l'attività di "bonifica" cinese. La capacità di ricorrere a mezzi proporzionati per rispondere rapidamente è una condizione importante affinché un messaggio deterrente sia efficace. Quanto più aggressive sono le provocazioni della "zona grigia" tanto più è possibile scoraggiarle perché possono essere identificate, attribuite e presentate come una minaccia grave agli interessi nazionali in maniera da rendere credibili i tentativi di dissuasione. La gradualità con cui si è arrivati a un nuovo status quo nel Mar Cinese Meridionale attraverso azioni incrementali fa sì che qualsiasi operazione militare diretta a bloccare o attaccare le isole artificiali cinesi possa invece apparire come una reazione sproporzionata ed eccessiva e rischi di ritorcersi contro chi si deve difendere ispirando invece simpatia per l'aggressore.

La "seconda" forza marittima

In Asia orientale si osserva il ricorso sempre più frequente alla guardia costiera piuttosto che alla marina militare per riaffermare le pretese di sovranità nelle acque contese. Ciò vale per Cina, Vietnam, Filippine, Taiwan e Malesia nel Mar Cinese Meridionale, per Cina e Giappone in riferimento alle isole Senkaku/Diaoyu e per Corea del Sud e Giappone nel caso delle isole Dokdo/Takeshima nel Mar Cinese Orientale così come per Singapore e Malesia nella disputa sull'isolotto di Pedra Branca.[3] In termini generali l'intervento della marina militare in un incidente o in una crisi tende ad alimentare i timori circa un imminente uso della forza, mentre il pattugliamento da parte delle guardie costiere potrebbe mitigare i rischi di un'escalation delle tensioni dato che operano spesso per coadiuvare la cooperazione inter-statale nell'ambito, ad esempio, delle missioni di ricerca e salvataggio e dovrebbe disporre di limitate capacità di combattimento.[4] In realtà, in Asia orientale la comparsa di tecnologie militari più avanzate sui cutter delle guardie costiere impiegate nelle missioni di pattugliamento nelle zone rivendicate da più stati complica la distinzione tra gli attori solitamente impegnati in operazioni di polizia e di difesa nazionale in tempo di pace.[5] Anche in questo caso si tratta di uno sviluppo pressoché dettato dalla condotta della Cina. Per soddisfare le ambizioni nazionaliste di riconquistare un ruolo

[3] Nel 2008 la Corte internazionale di giustizia ha riconosciuto la sovranità su Pedra Branca a Singapore mentre su Middle Rocks alla Malesia. Nel 2017 Kuala Lumpur ha presentato richiesta di revisione del pronunciamento citando nuovi documenti scoperti negli archivi britannici, ma il governo, eletto nel maggio 2018, ha successivamente informato la Corte della volontà di non procedere avviando invece dei colloqui bilaterali, tutt'oggi in corso, con le autorità di Singapore per la definizione dei confini marittimi nell'area.

[4] L. J. Morris, "Blunt Defenders of Sovereignty: The Rise of Coast Guards in East and Southeast Asia", *Naval War College Review*, vol. 70, n. 2, 2017.

[5] *Ibid.*

preminente nella regione, Pechino ha affidato, soprattutto nell'ultimo decennio, la sorveglianza dei territori marittimi rivendicati in larga parte alle forze sub convenzionali, ossia alle unità paramilitari come la Guardia costiera cinese in combinazione coi pescherecci. Quando Xi Jinping ha assunto la guida del Pcc nel novembre 2012 la guardia costiera non esisteva e le sue funzioni erano svolte da cinque diverse agenzie che competevano tra loro per l'allocazione delle risorse. Entro poche settimane dal suo insediamento la Marina dell'Epl è stata incaricata di trasferire una decina di navi ausiliarie a quella che sarebbe diventata la guardia costiera mentre accelerava la produzione di diverse nuove classi di navi da pattugliamento oceanico. Attualmente la Guardia costiera cinese è la più grande al mondo e sorpassa il totale degli scafi di tutti i vicini regionali. Secondo le stime del Dipartimento della Difesa statunitense la flotta delle grandi navi da pattugliamento della Guardia costiera cinese è più che raddoppiata superando attualmente i 130 scafi dotati per la maggior parte di strutture per elicotteri, cannoni ad acqua e cannoni tra i 30 mm e i 76 mm, inoltre, ha a disposizione 70 pattugliatori veloci per le operazioni offshore limitate e circa 1.000 motovedette costiere e fluviali.[6]

Con l'avvento di Xi la Guardia costiera cinese è stata potenziata oltre che sul piano del tonnellaggio delle navi su quello dell'efficienza operativa parallelamente alla modernizzazione della Marina. Nel marzo 2013 l'Assemblea nazionale del popolo ha approvato il piano di centralizzazione del controllo burocratico su quattro delle cinque agenzie di *law enforcement* marittimo, tra cui la neonata Guardia costiera, riunendole sotto l'Amministrazione statale oceanica, un organismo civile alle dipendenze del Ministero del territorio e delle risorse naturali. A distanza di cinque anni la sinergia tra i quattro corpi era ancora al di sotto delle aspettative, perciò nel 2018 il controllo sulla Guardia costiera è passato alla Polizia armata popolare a sua volta appena riorganizzata sotto la Commissione militare centrale.[7] Da corpo paramilitare marittimo la Guardia costiera cinese si trova all'interno della struttura di comando militare e il suo sviluppo come forza professionale è stato favorito dall'adozione di un quadro legislativo *ad hoc*. I due documenti chiave sono l'avviso emanato dalla Corte suprema del popolo e dalla Procura suprema del popolo nel 2020, che ha riconosciuto la giurisdizione della Guardia costiera cinese nei casi di criminalità marittima, e la prima legge sulla Guardia costiera cinese approvata durante la 25° riunione del Comitato permanente del 13° Congresso nazionale del popolo cinese il 22 gennaio 2021. A seguito del processo di riforma il mandato della guardia costiera è rimasto invariato così come il suo ruolo di principale forza cinese di *law enforcement* marittimo nelle aree contese che ora può svolgere per periodi lunghi con navi da pattugliamento più grandi e meglio equipaggiate.[8] Nel Mar Cinese Meridionale le missioni di monitoraggio da parte della Guardia costiera cinese sono compiute non solo a cadenza regolare, ma includono tattiche più aggressive, come gli speronamenti, rispetto al passato quando le navi che rilevavano la presenza di imbarcazioni straniere in attività ritenute "illegali" all'interno della "linea a nove tratti" si limitavano prevalentemente al richiamo verbale attraverso comunicazioni radio, per ribadire la sovranità cinese, fino ai tentativi di allontanamento con riflettori e cannoni ad acqua.[9] Tra il 2018 e il 2020 la guardia costiera ha anche scortato le navi cinesi lungo il confine occidentale della linea per condurre rilevazioni sismiche nella zona economica esclusiva del Vietnam, ha intimidito la Malesia per aver sfruttato le risorse dei fondali marini nella sua zona economica esclusiva vicino al confine sudorientale e ha affiancato i pescatori cinesi durante la pesca a

[6] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China", *Annual Report to Congress*, settembre 2020.
[7] Li Jiayao, "Enforcement powers of China Coast Guard expanded", *China Daily*, 23 giugno 2018.
[8] Ufficialmente le responsabilità della Guardia costiera cinese includono combattere la criminalità in mare, garantire la sicurezza marittima, sostenere lo sviluppo e lo sfruttamento delle risorse marine, proteggere l'ambiente marino, gestire la pesca, reprimere attività di contrabbando in mare. *Ibid*.
[9] K. Vu, "Vietnam protests Beijing's sinking of South China Sea boat", *Reuters*, 4 aprile 2020.

strascico nella zona economica esclusiva dell'Indonesia lungo il confine meridionale della linea.[10] Nonostante abbia impiegato un'ampia gamma di tattiche coercitive per raggiungere gli obiettivi strategici e operativi di Pechino, la Guardia costiera cinese si è astenuta dall'usare la forza armata contro le imbarcazioni straniere, ma la Legge entrata in vigore il 1° febbraio 2021 potrebbe potenzialmente incoraggiare sviluppi in senso contrario.[11] Un linguaggio molto ambiguo è riservato all'ipotesi di ricorrere all'artiglieria navale nel caso in cui la Guardia costiera cinese subisca un attacco con armi e "altri metodi pericolosi" o per impedire agli stranieri di violare la "sovranità, i diritti sovrani e i diritti giurisdizionali cinesi".[12] La mancanza di chiarezza vale soprattutto in relazione all'ambito di applicazione delle sue disposizioni alle "acque giurisdizionali" cinesi che nella versione finale della Legge non sono state specificate. Al contrario, la bozza della legge chiariva che dovevano essere incluse le "acque interne, mare territoriale, zone contigue, zona economica esclusiva e piattaforme continentali"; una specifica poi eliminata a seguito delle proteste da parte di varie cancellerie regionali. Se consideriamo il disegno di legge, e non il testo finale, unitamente a molteplici fonti cinesi si può concludere che Pechino rivendichi la giurisdizione su circa tre milioni di km^2 di spazio marittimo che includono il Golfo di Bohai, un'ampia sezione del Mar Giallo, il Mar Cinese Orientale fino al Canale di Okinawa comprese le acque intorno alle isole Senkaku/Diaoyu e tutte le acque all'interno della "linea dei nove tratti" (*jiu duan xian* 九段线, espressione cartografica delle sue rivendicazioni territoriali) nel Mar Cinese Meridionale.[13]

La "terza" forza marittima

La Milizia marittima cinese (Mmc) è l'altro attore accanto alla Guardia costiera cinese a difesa delle rivendicazioni marittime di Pechino con la Marina dell'Epl a supporto in caso di necessità. Il coinvolgimento delle milizie marittime nei vari incidenti nel Mar Cinese Meridionale e Orientale è stato documentato già a partire dallo scontro con il Vietnam per il controllo delle isole Paracel occidentali nel 1974, ma è dal 2015 che la Cina ha sviluppato una milizia a tempo pieno con unità più professionali, militarizzate e ben pagate fino a farla diventare il più grande contingente di questo tipo al mondo. Si tratta di pescatori ed equipaggi di navi civili che non avendo responsabilità di pesca si addestrano nelle diverse basi collocate lungo le province costiere sud-orientali per molteplici contingenze, in tempo di pace e di guerra, rispondono a una struttura militare di comando e controllo e svolgono attività di supporto militare a bordo dei pescherecci.[14] Un articolo cinese descrive in questo modo il ruolo delle milizie marittime: "Mettendosi in mimetica diventano soldati; togliendosi il camuffamento diventano pescatori rispettosi della legge".[15] Questo è il caso ad esempio delle centinaia di navi che sono arrivate nella zona contigua delle isole Senkaku durante l'incidente di pesca

[9] R. Fachriansyah e Fadli,"Indonesia talks sovereignty with China following foreign vessel controversy", *The Jakarta Post*, 14 settembre 2020.
[11] R.D. Martinson, "Gauging the real risks of China's new coastguard law", *Australian Strategic Policy Institute*, 23 febbraio 2021.
[12] *Ibid*.
[13] State Council Information Office of the PRC, "Speech by Comrade Xi Jinping at the Eighth Collective Study of the Political Bureau of the CPC Central Committee", 30 luglio 2013; Fu Chu, 1959 *cit*. in J.A. Cohen e Hungdah Chiu, *People's China and International Law*, Princeton: Princeton University Press, 1974, p. 484; State Council Information Office of the People's Republic of China, "Full Text: Diaoyu Dao, an Inherent Territory of China", 26 settembre 2019.
[14] C.M. Kennedy e A.S. Erickson, "China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA", *China Maritime Report No. 1*, China Maritime Studies Institute Center For Naval Warfare Studies - U.S. Naval War College, marzo 2017.
[15] "Military Subdistrict of Guangxi Strengthens Maritime Militia Construction, Increases Equipment Performance", *PLA Daily*, 6 gennaio 2014.

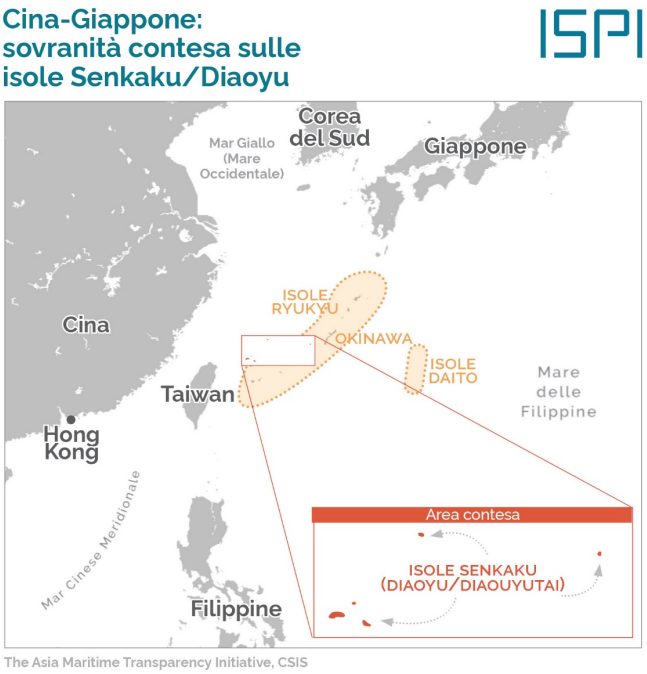
dell'agosto 2016 a bordo delle quali la Guardia costiera giapponese ha individuato "oltre 100 milizie marittime perché chiaramente identificabili da divise o uniformi militari e dal fatto che stessero dando ordini ai pescatori cinesi".[16] Pechino ha tentato di "civilizzare" l'espansione della protezione della sovranità per rafforzare le sue rivendicazioni giuridiche sugli altri reclamanti impiegando risorse ufficialmente non militari per riaffermare il controllo amministrativo sui territori contesi. La presenza della Mmc crea una dinamica destabilizzante per la controparte perché offusca la separazione tra comando civile e militare sulle risorse civili. Nel caso, per esempio, in cui le navi della Mmc portassero fuori rotta navi da guerra avversarie queste dovrebbero rispondere a tattiche ibride esibite da una nave nominalmente civile e l'eventuale successiva escalation evocherebbe l'immagine di un attacco militare contro un non combattente disarmato. È indicativo che la strategia marittima *Advantage at Sea,* pubblicata nel dicembre 2020 congiuntamente dalla Marina, dal corpo dei Marines e dalla Guardia costiera degli Stati Uniti, dedichi notevole spazio alla Mmc. Questo documento evidenzia la consapevolezza dei tre corpi navali statunitensi che per prevalere nella concorrenza strategica nello spazio marittimo Washington debba acquisire il vantaggio di operare efficacemente al di sotto della soglia del conflitto armato e quindi nella "zona grigia" del dominio marittimo in quanto non può più presumere di disporre del controllo assicurato in un ambiente marittimo conteso.[17]

Le isole Senkaku/Diaoyu

L'attenzione riservata alle tattiche cinesi di "zona grigia" più visibili nel Mar Cinese Meridionale ha talvolta messo in secondo piano quelle non meno destabilizzanti nel Mar Cinese Orientale: uno snodo critico in cui si concentrano le tensioni tra Cina e Giappone e che rappresenta una sfida rilevante anche per l'alleanza di sicurezza tra Tokyo e Washington. In quest'area sia la Cina sia il Giappone reclamano zone economiche esclusive (Zee) che si sovrappongono al pari delle loro zone di identificazione per la difesa aerea (*Air Defence Identification Zone*, ADIZ). A ciò si aggiunge la disputa sulle isole Senkaku (钓鱼岛 *Diaoyu Dao* in cinese) che si trovano a circa 330 km a sud-est della Cina e a circa 170 km a nord dell'isola di Ishigaki nella prefettura di Okinawa.[18] Il Giappone amministra gli otto affioramenti disabitati dal 1895 a eccezione del periodo dell'amministrazione statunitense di Okinawa dal 1950 al 1972. La Cina ne ha rivendicato ufficialmente la proprietà nel 1971, ma per Tokyo è una questione di sovranità su cui non è disposta a negoziare e per questo non ha mai riconosciuto ufficialmente la disputa. Accanto ai vantaggi economici derivanti dalle risorse ittiche e dai potenziali giacimenti di idrocarburi, il controllo di questi isolotti è una questione di orgoglio nazionale per entrambi, un fattore che alimenta il rischio di un conflitto scatenato da eventi accidentali dato che le forze aeree e della Guardia costiera cinese si introducono regolarmente nello spazio aereo giapponese e nelle acque territoriali vicino alle isole contese. Nel 2008 il Giappone ha accusato la Guardia costiera cinese di aver violato per la prima volta le acque territoriali giapponesi nelle isole Senkaku mentre la Cina ha risposto affermando che si trattava di acque territoriali cinesi. Le maggiori criticità sono arrivate nel 2010 e nel 2012 e le tensioni sono diventate più visibili anche all'opinione pubblica. Dopo lo scontro

[16] "尖閣諸島を襲う中国漁船に乗船する「海上民兵」の正体 [The True Colours of the Maritime Militia Embarked on the Chinese Fishing Vessels Attacking the Senkakus]", *Ironna Japan*, 13 ottobre 2016.
[17] U.S. Department of Defense (DoD), "Advantage at Sea: Prevailing with Integrated All-Domain Naval Power", 16 dicembre 2020.
[18] Il Giappone insiste sul fatto che a causa della sovrapposizione delle Zee il confine dovrebbe essere tracciato lungo la linea mediana tra Giappone e Cina, mentre la Cina sostiene che il confine debba essere conforme al requisito di 200 miglia nautiche definito dalla Convenzione delle Nazioni Unite sul diritto del mare (Unclos). La richiesta della Cina è inaccettabile per il Giappone non solo economicamente ma anche strategicamente perché in quel caso il confine cinese circonderebbe le isole di Okinawa che avrebbero così solo 20 miglia nautiche di acque territoriali.

nel 2010 tra i pescherecci cinesi e due navi della Guardia costiera giapponese, il nervosismo latente è sfociato a settembre di due anni più tardi a seguito della decisione del governo giapponese di acquistare tre fra queste isole da proprietari privati per impedire la vendita al governatore nazionalista di Tokyo Shintaro Ishihara che avrebbe turbato ulteriormente le relazioni con la Cina. Alla notizia, i cittadini cinesi delle città di primo e secondo livello sono scesi nelle strade e il governo ha definito l'acquisizione una flagrante violazione della sovranità cinese alla quale sarebbe stato necessario rispondere militarmente. La Cina ha utilizzato questi eventi per creare una "nuova normalità" sostituendo la pratica delle incursioni occasionali con passaggi frequenti vicino alle Senkaku delle navi della "seconda" e "terza" forza marittima cinese al fine di delegittimare la sovranità che Tokyo ha sostenuto attraverso l'esercizio del controllo amministrativo. Nei giorni successivi all'annuncio, due navi della China Marine Surveillance sono entrate entro le 12 miglia nautiche dando il via a una campagna di intrusioni intensificate nella zona contigua da parte delle navi cinesi di *law enforcement* marittimo che sono transitate nei mari territoriali per poche ore mantenendosi in contatto con gli ufficiali giapponesi per impedire l'insorgere di errori di calcolo e di incidenti. L'impressione era che alla Cina bastasse sostenere le sue rivendicazioni facendo transitare le imbarcazioni della Guardia costiera e della Milizia marittima piuttosto che lanciare azioni provocatorie contro le navi della Guardia costiera giapponese e indurle potenzialmente a mettere in atto misure aggressive per allontanare le navi cinesi. Nel dicembre 2015 Pechino ha inviato la prima nave armata in dotazione alla sua Guardia costiera e di fatto ha alzato la posta in gioco nonostante per la Cina si sia trattato semplicemente di un atto volto a bilanciare l'equilibrio degli armamenti dato che, fino a quel momento, aveva sostenuto che le navi disarmate della sua Guardia costiera fossero state inseguite dai cutter armati della Guardia costiera giapponese. Tra il 5 e il 9 agosto 2016 l'arrivo di 200-300 pescherecci cinesi e 15 navi della Guardia costiera cinese nella zona contigua intorno alle isole Senkaku ha prodotto una recrudescenza delle tensioni. Questa tattica definita come "sciame" di imbarcazioni ha messo a dura prova la capacità di risposta della Guardia costiera giapponese tanto da far supporre che, se riproposta nel caso di uno scontro, il Giappone sarebbe sopraffatto e incapace di far confluire un numero sufficiente di risorse per fronteggiare la controparte cinese.[19]



[19] J. Johnson, "Chinese Senkaku swarm tactic spells trouble for japan", *The Japan Times*, 7 agosto 2016.

Recentemente il *modus operandi* della Guardia costiera cinese è variato. Tra aprile e agosto 2020 le sue navi sono state avvistate nelle acque territoriali delle Senkaku per 111 giorni e hanno operato nella zona contigua ininterrottamente per 283 giorni fino a novembre; il periodo più lungo dall'acquisizione delle isole da parte del governo giapponese nel 2012.[20] Ciò suggerisce, secondo Patalano, che Pechino stia esercitando azioni di *law enforcement* non più limitate a segnalare la sua presenza nelle acque attorno alle isole ma stia sfidando attivamente il controllo giapponese entrando nella "seconda fase della triplice strategia di attrito cinese il cui obiettivo è quello di assumere il controllo esclusivo delle Senkaku".[21] Benché la Cina non abbia tentato di impossessarsi delle isole con la forza e si astenga in larga parte dal tipo di comportamento che persegue nel Mar Cinese Meridionale, le azioni della Guardia costiera cinese e della Mmc colpiscono direttamente l'integrità territoriale del Giappone. Finché Pechino manterrà questa competizione nell'ambito dell'esercizio di azioni di polizia marittima, il "vantaggio dell'iniziativa" resterà nelle mani del Pcc che potrà decidere se effettivamente sfidare lo status quo, limitare il rischio di un'escalation militare, oppure far ricadere sulle autorità giapponesi l'onere della risposta e guadagnare eventualmente una vittoria tattica sul fronte della narrazione.[22]

L'ADIZ cinese, sudcoreana e giapponese

Le azioni da parte delle navi cinesi di *law enforcement* marittimo a danno dell'integrità territoriale giapponese attorno alle Senkaku non sono l'unica sfida diretta che devono affrontare i funzionari giapponesi. La Cina ha anche intensificato la sua attività nello spazio aereo giapponese, soprattutto nella sezione occidentale e sudoccidentale dell'ADIZ del Giappone, dopo la prima violazione dello spazio aereo territoriale sulle isole Senkaku nel dicembre 2012 da parte di un aereo da pattugliamento. Tra il 2012 e il 2016, per rispondere alle incursioni cinesi, i caccia delle Forza aerea di autodifesa giapponese sono decollati più di 1.000 volte superando il record di 944 nel 1984 durante la Guerra fredda.[23] L'ADIZ è una designazione dello spazio aereo in cui i paesi cercano di monitorare il traffico per motivi di sicurezza nazionale. Queste zone si estendono tipicamente ben oltre i confini di uno stato per consentire l'identificazione e l'intercettazione di aeromobili che potrebbero essere una minaccia prima che raggiungano i suoi confini. La designazione delle ADIZ, che non sono formalmente riconosciute del diritto internazionale, ha avuto origine in Asia nordorientale sulla scia della seconda guerra mondiale e della guerra di Corea e sono state tracciate in gran parte dagli Stati Uniti seguiti dal Giappone e dalla Corea del Sud. Per molti anni le varie zone non si sono sovrapposte. La situazione è decisamente cambiata sul finire del 2013. A novembre di quell'anno la Cina ha ampliato la sua ADIZ nel Mar Cinese Orientale per includere le isole Senkaku generando una sovrapposizione con un'ampia porzione dell'ADIZ stabilita dal Giappone, suggerendo che la mossa sia stata progettata per rafforzare le pretese marittime e insulari di Pechino nonché per giustificare le attività aeree tese a difenderle. Washington e i suoi alleati regionali considerano l'ADIZ cinese come una provocazione in quanto dichiarata unilateralmente senza previa consultazione su un'area marittima contesa con il Giappone, una violazione del principio della libertà di sorvolo in alto mare prescritto nella Convenzione delle Nazioni Unite sul diritto del mare (Unclos), e temono che sia il preludio a un'ulteriore ADIZ cinese

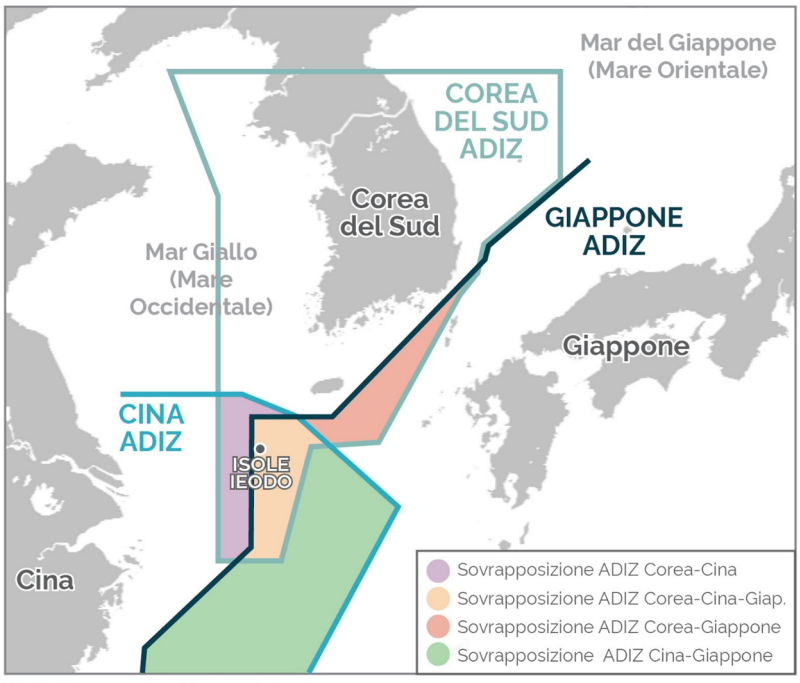
[20] J. Tsuruta, "The Chinese Coast Guard and the Senkaku: Activities of the last year suggest what the future might hold", *The Diplomat*, 30 dicembre 2020.
[21] A. Patalano, "What is China's Strategy in the Senkaku Islands?", *War on the Rocks*, 10 settembre 2020.
[22] *Ibid*.
[23] "Japan scrambled jets against approaching aircraft a record 883 times over nine months; most incidents involved China", *The Japan Times*, 21 gennaio 2017.

nel Mar Cinese Meridionale. Solo due giorni dopo, gli Stati Uniti hanno "salutato" l'ADIZ cinese attraversandola con un bombardiere B-52 con capacità nucleare senza previa comunicazione.

L'estensione dell'ADIZ cinese ha finito anche per includere un gruppo di rocce sommerse che i coreani chiamano Ieodo. La Corea del Sud ha risposto il mese successivo espandendo la propria ADIZ verso sud per includere Ieodo col risultato che l'ADIZ di Seoul si sovrappone a parte di quella cinese ma anche a quella giapponese. Nel 2019 il potenziale destabilizzante è diventato evidente quando i velivoli impegnati in un'esercitazione aerea congiunta russo-cinese hanno attraversato l'ADIZ sino-sudcoreana inducendo sia il Giappone sia la Corea del Sud a schierare i propri velivoli in risposta all'incursione. I piloti russi e cinesi hanno proseguito verso nord ma uno degli aerei russi ha volato all'interno dello spazio aereo territoriale di 12 miglia nautiche intorno a Dokdo/Takeshima, scogli amministrati dalla Corea del Sud ma rivendicati dal Giappone. Gli aerei sudcoreani hanno sparato 360 colpi di avvertimento e hanno protestato in maniera molto decisa contro l'incursione. Il Giappone che era ugualmente furioso per le azioni della Russia ha criticato aspramente anche la Corea del Sud per aver sparato contro l'aereo russo nel proprio spazio aereo. L'anno successivo, gli aerei russi e cinesi hanno evitato di attraversare lo stesso spazio aereo territoriale. Gli accessi senza notifica da parte dell'aviazione cinese nell'ADIZ sudcoreana sono aumentati da 50 a 140 tra il 2016 e il 2018 mentre nel 2019 sono scesi a 25. Al fine di prevenire incidenti militari i due paesi hanno convenuto di istituire nuove linee di comunicazione militare dirette, passate da una sola nel periodo 2015-2019 a cinque nel 2021.[24] Nel 2019, per esempio, l'esercito sudcoreano ha contattato un aereo cinese che stava entrando nell'ADIZ sudcoreana e ha fornito le sue informazioni di volo attenuando, solo parzialmente, i timori di Seoul relativamente alle intenzioni cinesi.

La sovrapposizione delle zone di identificazione per la difesa area (ADIZ) nel Mar cinese orientale

ISPI



FONTE: Congressional Research Service

[24] "S. Korea, China agree to establish two more military hotlines", *Yonhap*, 2 marzo 2021.

La risposta giapponese e le implicazioni per l'alleanza con gli Stati Uniti

Il governo giapponese ha iniziato a utilizzare il termine "zone grigie" nel 2010, un anno peraltro simbolico in cui Pechino ha scalzato Tokyo come seconda economia mondiale, per riferirsi a "incidenti armati che non raggiungono i livelli di un attacco su vasta scala".[25] Per il Giappone queste situazioni sono il prodotto prevalentemente dell'"assertività reattiva" della Cina.[26] Nel più recente Libro Bianco sulla difesa, Tokyo ha descritto la natura della minaccia cinese alla sua sicurezza con toni estremamente duri ribadendo che le crescenti attività marittime a sostegno delle costanti rivendicazioni cinesi sulle isole Senkaku "minano lo status quo".[27] Dal punto di vista delle risorse in campo il governo sta rafforzando la difesa della catena di isole sudoccidentali dell'arcipelago giapponese attraverso la più ingente concentrazione di truppe di terra, missili e strutture seguendo un approccio multi fase alla pianificazione di emergenza nell'eventualità in cui le tensioni causate dalle incursioni cinesi attorno alle Senkaku subiscano un'escalation.[28] A livello legislativo, invece, perdura un *vacuum* relativo a ciò che costituisce una circostanza di "zona grigia". La questione avrebbe dovuto essere al centro della legislazione sulla sicurezza adottata nel settembre 2015 che, tuttavia, si è concentrata principalmente sull'uso limitato del diritto all'autodifesa collettiva. Ma non solo. Il peculiare sistema di sicurezza giapponese, che ha mantenuto una chiara separazione tra le risorse militari e quelle civili, ha di fatto ostacolato l'adozione di un quadro giuridico volto, da un lato, a regolare il coordinamento tra la Guardia costiera giapponese, l'agenzia di *law enforcement* puramente civile posta sotto il Ministero del territorio, delle infrastrutture, dei trasporti e del turismo, e la componente militare rappresentata dalla Forza marittima di autodifesa, e dall'altro, ad ampliare le regole di ingaggio di queste ultime.[29] Qualora il governo giapponese ritenga che una missione di sorveglianza e sicurezza in prossimità dei confini marittimi e delle isole remote ecceda le capacità della Guardia costiera giapponese, la Forza marittima di autodifesa può essere inviata a supporto e ciò "non costituirebbe un'azione militare ortodossa ma un'operazione di *law enforcement*" secondo l'articolo 82 della Legge sulle Forze di autodifesa.[30] Per il governo giapponese quindi queste operazioni a garanzia della sicurezza marittima dovrebbero essere considerate un'attività non di combattimento ma di polizia marittima portata avanti da forze più capaci per prevenire un'escalation militare.[31] Di opinione nettamente opposta sarebbe Pechino per cui qualsiasi intervento in una situazione di "zona grigia" da parte della Forza marittima di autodifesa sarebbe un'azione unilaterale di escalation militare attribuibile al governo giapponese.[32] Questo è il motivo per cui l'"assertività reattiva" cinese complica i calcoli di Tokyo che è costretta a rispondere con un "sistema di sicurezza binario" in cui il coordinamento tra le proprie agenzie marittime non è ottimale e questo penalizza la risposta a salvaguardia dell'integrità territoriale giapponese nel Mar Cinese Orientale.[33]

---

[25] N. Kubo, L. Sieg, e P. Stewart, "Japan, U.S. Differ on China in Talks on 'Grey Zone' Military Threats", *Reuters,* 10 marzo 2014.
[26] Ministry of Defense of Japan, "National Defense Program Guidelines for FY 2014 and beyond", 2013.
[27] Ministry of Defense of Japan, "Defense of Japan", *Annual White Paper*, 2020.
[28] J. Ryall, "Japan's ground troops to get transport ships amid concerns over China's military build-up in Indo-Pacific", South China Morning Post, 15 febbraio 2021.
[29] C. Pajon, "Japan's Coast Guard and Maritime Self-Defense Force in the East China Sea: Can a Black-and-White System Adapt to a Gray-Zone Reality?", *Asia Policy*, n. 23, 2017.
[30] K. Furuya, "Maritime Security: The Architecture of Japan's Maritime-Security System in the East China Sea", *Naval War College Review*, vol. 72, n. 5, 2019, p. 4.
[31] Queste operazioni si sono verificate finora solo in tre occasioni: per inseguire una nave spia nordcoreana nel 1999, in risposta all'incursione di un sottomarino cinese nelle acque territoriali giapponesi nel 2004 e per condurre operazioni antipirateria nel Golfo di Aden nel 2009.
[32] C. Pajon (2017), p. 123.
[33] *Ibid.*

Nel corso del tempo è probabile che la capacità del Giappone di contrastare regolarmente la minaccia proveniente dalla Cina sarà sottoposta a ulteriori pressioni. Oltre ai necessari adeguamenti nella composizione delle forze militari giapponesi e nell'interoperabilità tra burocrazie militari e civili, gli sforzi giapponesi dovranno concentrarsi sul coordinamento interno all'alleanza di sicurezza con gli Stati Uniti. Da tempo negli incontri Track 1.5[34] i funzionari sudcoreani e giapponesi esprimono ai colleghi statunitensi la forte preoccupazione che le sfide della "zona grigia" possano erodere la credibilità degli impegni statunitensi. [35] L'articolo 5 del Trattato di sicurezza col Giappone impegna gli Stati Uniti a intervenire in caso di un "comune pericolo" rappresentato da "un attacco armato contro i territori sotto l'amministrazione del Giappone". Sebbene il Giappone si assuma la responsabilità primaria della propria difesa, in caso di un conflitto armato significativo con la Cina potrebbe invocare la disposizione del Trattato e chiedere l'assistenza di Washington. Dopo che le tensioni sino-giapponesi sulle Senkaku sono esplose nel 2012 il Congresso degli Stati Uniti ha ribadito il sostegno retorico al Giappone inserendo nel Piano di difesa nazionale per il 2013 un Atto di autorizzazione che stabilisce tra l'altro che "l'azione unilaterale di una terza parte non influirà sul riconoscimento da parte degli Stati Uniti dell'amministrazione giapponese sulle isole Senkaku".[36] Dall'amministrazione Nixon in poi gli Stati Uniti hanno chiarito che il Trattato include la questione delle isole e il presidente Obama ha aggiunto che gli Stati Uniti "non credono che [lo status delle isole Senkaku] debba essere soggetto a modifiche unilaterali".[37] Dopo la telefonata di Biden appena insediatosi alla Casa Bianca al primo ministro Suga, in cui il presidente ha ribadito "l'impegno incrollabile a difesa del Giappone ai sensi dell'articolo 5 del nostro trattato di sicurezza, che include le isole Senkaku", il Segretario alla Difesa Austin ha aggiunto che "gli Stati Uniti si oppongono a mosse unilaterali per cambiare lo status quo". Ciò non ha comunque alterato la contestuale neutralità del governo statunitense in merito a chi spetti la sovranità sulle isole Senkaku.[38]

Fino a oggi l'alleanza di difesa tra gli Stati Uniti e il Giappone sembra aver scoraggiato Pechino dal lanciare aggressioni convenzionali nel Mar Cinese Orientale ma le provocazioni a danno della sovranità e degli interessi nazionali giapponesi sono in rapido aumento e con esse il grado di tensione e sfiducia tra i vicini asiatici che preoccupa i due alleati, come confermato durante i colloqui di difesa "2+2" nel marzo 2021.[39] La possibilità che una collisione accidentale o deliberata degeneri rapidamente resta alta anche a causa del limitato successo da parte giapponese e cinese di concordare meccanismi condivisi per la gestione degli incidenti in mare o nei cieli. Il carattere mutevole delle operazioni nella "zona grigia" rende più difficile raggiungere un consenso tra Tokyo e Washington su ciò che costituisce un attacco armato. Nell'eventualità in cui il Giappone non possa attivare l'articolo 5 del Trattato probabilmente emergerebbero alcuni dei vincoli logistici, giuridici e politici dell'alleanza bilaterale così come le differenze tra le rispettive legislazioni nazionali circa la definizione di ciò che costituisce un atto di guerra o un attacco armato e tutto ciò complicherebbe la formulazione di una risposta congiunta. La principale sfida per il Giappone e gli Stati Uniti resta quella di cooperare efficacemente anche al di

[34] L'espressione "Track 1.5" si riferisce ai colloqui a porte chiuse tra funzionari governativi, che partecipano in veste non ufficiale, ed esperti non governativi per favorire la costruzione di fiducia tra le parti di un processo diplomatico ufficiale (Track 1) ed eventualmente incorporare nei negoziati gli input provenienti dalla società civile.
[35] J.L. Schoff e P.K. Lee, "Sustaining Strong Partnerships: The First Trilateral Dialogue Initiative (TDI) Workshop", *Carnegie Endowment for International Peace*, aprile 2019; B. Glosserman, "Struggling with the Gray Zone: Trilateral Cooperation to Strengthen Deterrence in Northeast Asia", *Asia, Issues &* Insights, vol. 15*,* n. 13*,* 2015.
[36] Congress of the United States of America, "National Defense Authorization Act for Fiscal Year 2013", 2, gennaio 2013.
[37] "Obama Asia tour: US-Japan treaty 'covers disputed islands'", *BBC*, 24 aprile 2014.
[38] J. Johnson, "New U.S. defense chief confirms Senkakus fall under security treaty", *Japan Times*, 24 gennaio 2021.
[39] Ministry of Foreign Affairs of Japan, "Joint Statement of the U.S.-Japan Security Consultative Committee (2+2)", 16 marzo 2021.

fuori dell'impegno previsto dall'articolo 5 soprattutto in seguito agli sviluppi connessi all'impiego della Guardia costiera cinese e agli effetti che la Legge in vigore da febbraio 2021 potrebbe produrre.

IL DOMINIO CIBERNETICO NELLA STRATEGIA ASIMMETRICA NORDCOREANA

Fin dalle origini la Corea del Nord ha investito massicce risorse nello sviluppo di capacità militari asimmetriche che colmassero il divario in termini convenzionali con l'alleanza di sicurezza formata da Stati Uniti e Corea del Sud. Per il regime della famiglia Kim l'acquisizione e l'avanzamento del programma nucleare e missilistico rappresentano una garanzia di sopravvivenza per la nazione e quindi per la leadership stessa, due concetti che nel contesto nordcoreano coincidono.[40] La percezione della minaccia che ha reso necessario proseguire nella direzione del nucleare si è mantenuta immutata e costante così come è stata formulata da Kim Il Sung fino all'attuale terza generazione di leader. Sul fronte esterno la principale fonte di insicurezza per il regime è rappresentata dallo stato di costante "assedio" a cui Pyongyang si sente sottoposta fin dalla guerra di Corea (1950-53) e contro cui ha ripetutamente adottato un atteggiamento aggressivo a scopo di deterrenza. Sul fronte interno la minaccia è stata invece associata al trasferimento del potere dal leader ai suoi successori.[41] In questo quadro si inseriscono a partire dai primi anni Novanta anche le tattiche e le strategie riservate al dominio cibernetico che con costi economici più contenuti ampliano le opzioni potenzialmente a disposizione del regime nordcoreano per danneggiare le risorse militari o gli obiettivi socio-economici chiave degli stati co-responsabili della "politica ostile", così definita costantemente dalla propaganda ufficiale, a guida statunitense.[42] Nel 2013 l'Agenzia di intelligence sudcoreana ha riportato durante uno dei consueti briefing all'Assemblea nazionale una dichiarazione attribuita a Kim Jong Un secondo cui "la guerra cibernetica è una spada multiuso che così come le armi nucleari e i missili garantisce all'Esercito popolare nordcoreano la capacità di colpire spietatamente [l'avversario]".[43] Accanto all'obiettivo di mettere in discussione le logiche della deterrenza tradizionale con potenziali nuove modalità di aggressione, le conoscenze e gli strumenti sviluppati in ambito informatico sono stati impiegati dal regime nordcoreano principalmente per evadere le sanzioni unilaterali e multilaterali e incamerare risorse finanziarie da investire nel programma nucleare e missilistico così come per raccogliere informazioni sensibili a scopo di spionaggio. Sul finire degli anni Duemila i profitti derivanti tra gli altri dalla produzione e dal commercio di stupefacenti, dal contrabbando di avorio e dalla contraffazione di denaro sono diventati insufficienti per resistere alla morsa di un regime sanzionatorio in espansione e l'attenzione della Corea del Nord è caduta in particolare sul settore della criminalità informatica. Il regime nordcoreano impiega almeno dal 2015 gli strumenti informatici per eludere le sanzioni internazionali incluse quelle relative all'embargo sulle armi come nel caso degli attacchi all'*Indian Space Research Organization* e la *Kudankulam Nuclear Power Plant* e alla

[40] Per un approfondimento sul programma nucleare e missilistico nordcoreano si veda: A. Berkofsky e F. Frassineti, "La sfida nordcoreana agli equilibri internazionali", *Osservatorio di Politica Internazionale*, 2018.
[41] Y. Kim, *North Korean Foreign Policy: Security Dilemma and Succession*, Lanham, MD: Lexington Books, 2010.
[42] "Kim Jong Un Supervises Test-launch of Inter-continental Ballistic Rocket Hwasong-14", *Kcna*, 5 luglio 2017.
[43] È utile ricordare ai fini di questa analisi che non tutte le aggressioni consumate attraverso le reti di telecomunicazioni o i sistemi informatici di un paese possono essere qualificate come "guerra cibernetica" (*cyberwarfare*). Secondo Cadoppi et *al*. (2019) la "cyberwarfare" si configura quando l'impiego di tecniche marcate di intrusione o sabotaggio delle risorse informatiche e fisiche di un paese avversario è associato a una manifesta attività bellica convenzionale col fine di compromettere le difese, il funzionamento e la stabilità economica e socio-politica del nemico.

sudcoreana *Daewoo Shipbuilding & Marine Engineering Co. Ltd*.[44] Accanto ai continui trasferimenti illeciti da nave a nave dei beni sottoposti a sanzione, in primis del carbone che rappresenta il fulcro dell'export nordcoreano, la diffusione della valuta digitale ha aperto nuove vie per aggirare i vincoli imposti dalla comunità internazionale e accumulare riserve di valuta estera. Le unità informatiche della Corea del Nord hanno mostrato una notevole diversità in termini di capacità ed esperienza includendo gli attacchi *ransomware*,[45] la diffusione di reti di computer infettati da un malware che permette ai criminali informatici di prenderne il controllo (*botnet*) ed eseguire determinate operazioni come l'estrazione illegale di criptovalute (*mining*) con particolare interesse per gli Altcoin,[46] e le operazioni multinazionali contro gli sportelli di prelievo automatici. Indubbiamente il successo di queste operazioni trae vantaggio dalle vulnerabilità nei sistemi di sicurezza delle istituzioni finanziarie prese di mira, ma in alcuni casi, anche dal disincentivo da parte delle stesse a notificare le violazioni subite dalle proprie reti informatiche per non esporsi a responsabilità legali e per non minare la fiducia e il valore di mercato.

La gamma di tattiche, tecniche e procedure

La prima generazione di software malevoli attribuiti alla Corea del Nord risale al periodo 2007-2012 diffusi attraverso attacchi informatici come "Operation Flame", "1Mission", "Operation Troy" e "Ten Days of Rain" che hanno colpito principalmente agenzie governative, banche e grandi società sudcoreane manipolando le reti Internet attraverso una serie di attacchi *distibuted denial-of-service* (DDoS). Il 2013 è stato particolarmente intenso per la resilienza del sistema informatico sudcoreano in concomitanza con una recrudescenza delle tensioni nella penisola coreana seguita al giro di vite sulle sanzioni del Consiglio di Sicurezza dell'Onu contro Pyongyang (ris. 2087 e 2094), al sorvolo dei bombardieri B-2 e B-52 sulla Corea del Sud nell'ambito delle consuete esercitazioni congiunte con gli Stati Uniti e al dispiegamento di un nuovo sistema di difesa missilistica THAAD nella vicina Guam. Pyongyang ha reagito con dichiarazioni al vetriolo contro gli Stati Uniti, la Corea del Sud e il Giappone minacciando di usare le sue armi nucleari contro obiettivi statunitensi. Tredici giorni dopo l'adozione da parte del Consiglio di Sicurezza (CdS) della seconda risoluzione anche gli attacchi informatici contro la Corea del Sud si sono intensificati. L'operazione "Dark Seoul" ha colpito sei tra le maggiori banche e aziende della comunicazione sudcoreane, con danni per 800 milioni di dollari, e ha sospeso o ritardato le operazioni nel sistema finanziario del paese per dieci giorni; solo il 10 per cento dei siti web presi di mira aveva ripreso a funzionare entro due giorni. A questo si è aggiunta una campagna di spionaggio informatico ribattezzata "Kimsuky" contro gli istituti di ricerca e le aziende private unitamente a vari attacchi DDoS.[47] L'operazione "Kimsuky" ha segnato l'inizio di una seconda fase in cui le attività informatiche malevoli attribuite alla Corea del Nord si sono concentrate sullo spionaggio informatico in particolare verso le strategie e le capacità militari della Corea del Sud con un grado di avanzamento tecnico superiore ai precedenti DDoS. Caratteristiche simili a "Kimsuky" sono state riscontrate nel furto a danno della *Korea Hydro and Nuclear Power* (KHNP) a cui sono stati sottratti documenti sui reattori nucleari e quasi sei mila email truffa (*phishing*) sono state inviate ai suoi

[44] UN Panel of Experts (2018), *Final report of the Panel of Experts submitted pursuant to resolution 2345 (2017)*, 8 marzo 2018, par. 119; UN Panel of Experts (2021), *Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 4 marzo 2021, par. 121.
[45] Il termine inglese *ransomware* nasce dalla contrazione delle parole *ransom* (riscatto) e *malware* (software maligno).
[46] Gli Altcoin sono valute virtuali meno popolari dei Bitcoin ma che offrono maggiore anonimato e rapidità nei trasferimenti.
[47] J.A.P. Marpaung, HJ Lee, "Dark Seoul Cyber Attack: Could it be worse?", CISAK Conference, 12 maggio 2013; S.H. Choe, "South Korea Blames North for June Cyberattacks", *The New York Times*, 16 luglio 2013.

dipendenti per alterare il funzionamento dell'infrastruttura informatica a sostegno della rete elettrica nazionale. Successivamente, un'importante operazione di spionaggio ha preso di mira i computer di tre membri dell'Assemblea nazionale e undici assistenti governativi e i cellulari di quaranta funzionari sudcoreani.[48] Nel 2016 dopo la scoperta, in ritardo, dell'attacco subito dalla *Daewoo Shipbuilding & Marine Engineering Co., Ltd*, con cui sono stati rubati alcuni documenti contenenti informazioni sulla tecnologia di costruzione dei sistemi d'arma e le valutazioni di navi e sottomarini, le autorità militari di Seoul si sono rese conto che il data centre del Comando di difesa cibernetico era stato violato. Gli oltre 235 GB di dati classificati esfiltrati includevano il piano operativo OPLAN 5015 per la "decapitazione" del leader nordcoreano, e parte del piano operativo OPLAN 5027 sviluppato congiuntamente con gli Stati Uniti contro una possibile offensiva nordcoreana a sud del 38° parallelo.[49] Le operazioni informatiche offensive attribuite alla Corea del Nord nel 2016 hanno mostrato, come nel 2013, particolare aggressività contestualmente al peggioramento dei rapporti con la comunità internazionale innescato a gennaio dal primo dei due test nucleari effettuati in quell'anno da Pyongyang.

Nel frattempo le operazioni cibernetiche avevano già superato i confini della penisola coreana con *modus operandi* e obiettivi diversificati. La sfida nordcoreana alla sicurezza cibernetica è stata portata all'attenzione del grande pubblico nel 2014 dall'operazione per bloccare l'uscita del film *The Interview* prodotto da *Sony Pictures Entertainment* e considerato dalla propaganda nordcoreana come un insulto al leader Kim Jong Un. Il gruppo di attaccanti denominati "Guardiani della pace", nominalmente un'entità indipendente ma ritenuta agire nell'interesse del regime di Pyongyang, ha cercato di impedire, senza riuscirci, l'uscita della pellicola mettendo fuori uso il 70 per cento dei terminali dell'azienda e rendendo accessibili le comunicazioni interne e personali dei dipendenti e dei dirigenti. Nello stesso anno ai gruppi di attaccanti sponsorizzati dal regime nordcoreano è stata attribuita la penetrazione nel circuito di banche collegate al sistema di messaggistica finanziaria globale SWIFT nel tentativo di trasferire 951 milioni di dollari dalla Banca centrale del Bangladesh a conti nello Sri Lanka e nelle Filippine. Da quel momento la Corea del Nord è stata associata a una serie di attacchi informatici mirati specificamente a guadagni finanziari illeciti presumibilmente per sopportare l'aumentata pressione sanzionatoria sul paese per ostacolare il suo programma di armi nucleari e missilistiche. Il periodo 2016-17 è stato infatti uno spartiacque per le sanzioni multilaterali dell'Onu che hanno conosciuto una evoluzione in termini sia di portata sia di complessità, con caratteristiche notevolmente differenti rispetto a quelle in vigore dal 2006. Il CdS è stato influenzato dagli sviluppi intercorsi nel regime di sanzioni imposte alla Corea del Nord dagli Stati Uniti. Nel gennaio 2015 il presidente Obama ha firmato l'Ordine esecutivo 13687 per autorizzare il governo statunitense a imporre sanzioni economiche nei confronti di persone fisiche e giuridiche nordcoreane in risposta all'attacco alla *Sony Pictures Enterprise* "senza dover più sottostare al vincolo di dimostrare che tali soggetti avessero contribuito materialmente alle attività di proliferazione".[50] Similmente i round sanzionatori approvati dal CdS a partire dalla risoluzione 2270 del marzo 2016 hanno cercato di incidere maggiormente sulla capacità di Pyongyang di accedere al sistema finanziario internazionale e sulle sue principali esportazioni di materie prime oltre che, come le precedenti sanzioni, paralizzare alcune componenti dell'economia nordcoreana relative al programma nucleare e balistico. Tra gli attacchi che sono stati

[48] P. Hancocks e K.J. Kwon, "North Korea hacked government officials' smartphones, South Korea says", *CNN,* 8 marzo 2016.
[49] K., Choi, "N. Korea likely hacked S. Korea Cyber Command: Military", *Yonhap News*, 6 dicembre 2016.
[50] A. Berger, "A House without Foundations: The North Korea Sanctions Regime and its Implementation", *RUSI Whitehall Report 3-17*, giugno 2017.

scoperti e attribuiti alla Corea del Nord è stato osservato un aumento del numero e dell'entità delle operazioni di spionaggio informatico rispetto al periodo precedente il 2016 e "almeno cinque attacchi [cyber] di successo contro gli scambi di criptovaluta in Asia tra gennaio 2017 e settembre 2018 con un guadagno totale di 571 milioni di dollari".[51] La Corea del Nord è ancora la principale indiziata per quello che probabilmente è stato il più grande furto di criptovalute nella storia (534 milioni di dollari in monete digitali NEM) subito nel 2018 dalla principale piattaforma giapponese per lo scambio di criptovalute *Coincheck*.[52] Si può concludere che i furti informatici siano diventati parte integrante della strategia di sopravvivenza della Corea del Nord anche se affinché questi bottini diventino disponibili per l'uso da parte del regime devono essere riciclati per nasconderne la provenienza. Nel caso della rapina alla Banca centrale del Bangladesh, da cui gli attaccanti hanno sottratto alla fine 80 milioni di dollari, è stata necessaria la conversione dei fondi rubati in *fiches* da casinò nelle Filippine e a loro volta in contante non rintracciabile.[53]

Il più allarmante degli attacchi informatici attribuiti ai nordcoreani ad oggi resta il *ransomware WannaCry* che nel 2017 ha infettato circa 200.000 terminali in oltre 150 paesi attraverso il sistema operativo Microsoft Windows 7 chiedendo alle vittime riscatti per diverse centinaia di dollari in Bitcoin per recuperare i loro dati. Il servizio sanitario nel Regno Unito è stato particolarmente colpito ed è stato costretto a deviare il percorso delle ambulanze, cancellare migliaia di appuntamenti e interventi chirurgici e trasferire dalle strutture interessate i pazienti in condizioni gravi. Gli investigatori della *National Crime Agency* britannica in collaborazione con l'FBI hanno trovato sorprendenti somiglianze con le violazioni ai danni della Banca centrale del Bangladesh e della *Sony Pictures Entertainment*. Ciò è emerso anche dalla documentazione a sostegno del procedimento penale a carico del cittadino nordcoreano Park Jin Hyok incriminato nel 2018 per il suo "coinvolgimento in una cospirazione volta a condurre molteplici attacchi informatici distruttivi in tutto il mondo perché ritenuto membro di una società di facciata del governo nordcoreano, *Chosun Expo Joint Venture* legata al gruppo Lazarus/APT 38" a cui il Dipartimento di Giustizia degli Stati Uniti ha attribuito la creazione del malware utilizzato negli attacchi citati.[54] Park è stato nuovamente incriminato nel febbraio 2021 insieme ad altri due nordcoreani, anch'essi affiliati al Lazarus Group e collegati a una rete globale di riciclaggio di denaro.[55]

L'infrastruttura Ict e il comando delle operazioni cibernetiche

Per la leadership di Pyongyang la scienza e la tecnologia hanno rivestito un ruolo fondamentale per la costruzione dello stato e la sicurezza nazionale; dopo soli sette anni dalla sospensione del conflitto il paese già vantava l'assemblaggio del primo computer in anticipo di tredici anni sul rivale sudcoreano.[56] Negli anni Ottanta sono state poste le fondamenta delle reti e delle capacità informatiche della Corea del Nord, sulla scia di quanto Kim Il Sung aveva visto nella Germania Est nel 1984, con una particolare attenzione al ruolo dell'istruzione e della formazione a sostegno degli obiettivi del partito

[51] UN Panel of Experts (2019), *Final report of the Panel of Experts submitted pursuant to resolution 2407 (2018)*, 5 marzo 219, par. 114.
[52] "North Korea Suspected in Coincheck", *Nikkei Asian Review*, 6 febbraio 2018.
[53] S. Quadir, "Bangladesh to sue Manila bank over $81 million cyber heist: cenbank governor", *Reuters*, 30 gennaio 2019.
[54] U.S. Department of Justice (DOJ), "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions", 6 settembre 2018.
[55] U.S. Department of Justice (DOJ), "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe", 17 febbraio 2021.
[56] K.M. Ko, *North Korea's IT Strategy*, Seoul: Communication Books, 2004, pp. 100-101.

appoggiandosi anche in questo ambito all'assistenza tecnica sovietica.[57] L'estate del 1997 ha segnato un altro passaggio chiave con l'avvio dell'intranet nazionale (*kwangmyeong*), uno degli strumenti attraverso cui il regime esercita un controllo capillare sulla diffusione delle informazioni nel paese permettendo solamente a un ristretto gruppo di accedere alla rete Internet globale.[58] Le unità informatiche nordcoreane e i gruppi di attaccanti sponsorizzati dal regime hanno fatto molta strada dalla fondazione del *Korea Computer Center* nel 1990 quando l'infrastruttura informatica del paese era nella migliore delle ipotesi rudimentale, per quanto l'istituto sia tuttora il fulcro delle operazioni informatiche della Corea del Nord. Fonti del governo statunitense ritengono che il regime disponga di oltre 7.000 unità operative nel dominio cibernetico e stimano che il volume delle attività da e verso le reti nordcoreane sia aumentato del 300 per cento dal 2017.[59]

Le attività nordcoreane nel cyberspazio sono conformi agli orientamenti e alle direttive del Partito dei lavoratori di Corea. L'esecuzione e il controllo delle operazioni informatiche è suddiviso tra lo Stato maggiore dell'Esercito popolare coreano e il *Reconnaissance General Bureau*. All'interno delle forze armate l' *Electronic Warfare Bureau* gestisce le operazioni di guerra elettronica mentre un dipartimento di recente istituzione è stato presumibilmente incaricato di accelerare l'integrazione delle capacità informatiche offensive nelle operazioni militari convenzionali per tenere in scacco le infrastrutture critiche dell'avversario e migliorare le capacità informatiche difensive dei sistemi di comando e controllo delle forze armate.[60] I primi segnali importanti dell'attivismo cibernetico malevolo riconducibile al regime nordcoreano risalgono, come detto, agli anni intorno al 2009 quando tutti i servizi di intelligence e di sicurezza interna, incluse le operazioni speciali e informatiche, sono stati unificati nel *Reconnaissance General Bureau*. Il fatto che quest'ultimo sia indipendente dall'Esercito popolare e che dal 2016 riferisca direttamente al più alto organo decisionale del regime, la Commissione per gli affari di stato presieduta da Kim Jong Un, suggerisce che il dominio cibernetico non sia concepito dal regime unicamente in termini di obiettivi militari.[61] Nel 2013 il *Reconnaissance General Bureau* ha istituito la Unit 180 incaricata inizialmente di colpire le istituzioni finanziarie internazionali per estrarre valuta estera a sostegno dei programmi nucleari e balistici e poi assegnata agli scambi di criptovalute, lasciando che sia la Unit 91 ad acquisire le tecnologie necessarie a perfezionare l'arsenale non convenzionale nordcoreano e a sottrarre informazioni confidenziali soprattutto alle agenzie governative sudcoreane.[62] L'organizzazione principale responsabile della guerra informatica nel *Reconnaissance General Bureau* secondo l'esercito statunitense è la Unit 121 che disporrebbe di almeno 1.000 hacker d'élite, arrivati ogni anno dal Mirim College, oltre a 6.000 membri molti dei quali operano da altri paesi come Bielorussia, Cina, India, Malesia e Russia.[63] In occasione della parata militare del 10 ottobre 2020 i media statali della Corea del Nord hanno confermato la fondazione di una nuova università scientifica e tecnologica che non potrà che

---

[57] D.A. Pinkston, "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Sŏn'gun Era", *Georgetown Journal of International Affairs*, vol. 17, n. 3, 2016, p. 62.
[58] *Ibid.*
[59] U.S. Department of Health and Human Services, "North Korean Cyber Activity", 25 marzo 2021.
[60] J. Jun, S. LaFoy, E. Sohn, *North Korea's Cyber Operations: Strategy and Responses*, Washington, D.C., Center for Strategic and International Studies, 2015, pp. 31-32.
[61] *NK Leadership Watch,* "National Defense Commission", 24 settembre 2016; M. Ha e D. Maxwell, "Kim Jong Un's 'All-Purpose Sword: North Korean Cyber-Enabled Economic Warfare", *Foundation for Defense of Democracies*, 3 ottobre 2018.
[62] K.J. Young, J.I. Lim e K.G. Kim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", Conference Paper, *11th International Conference on Cyber Conflict*, 28-31 maggio, 2019.
[63] U.S. Department of the Army, "North Korean Tactics", *Army Techniques Publication (ATP) 7-100 series*, luglio 2020.

approfondire la collaborazione informatica e tecnologica tra le forze civili e militari.[64] È noto inoltre che gli studenti nordcoreani meritevoli e appartenenti alle famiglie più vicine al regime studino spesso nelle migliori istituzioni cinesi, ad esempio, come l'*Harbin Institute of Technology* dove possono familiarizzare con la tecnologia avanzata non disponibile nel loro paese d'origine a causa delle sanzioni internazionali. Il governo di Pechino continua a stringere relazioni accademiche ufficiali con istituzioni accademiche nordcoreane affiliate all'esercito anche nel quadro di accordi di cooperazione e istruzione, come quello rinnovato recentemente per il decennio 2020-2030, per rafforzare i partenariati accademici e gli scambi di studenti post-laurea, che potrebbero però favorire anche le attività informatiche illegali nordcoreane.

I gruppi di attaccanti e il problema dell'attribuzione

Il vantaggio principale di Pyongyang è l'incertezza di cui beneficia chiunque operi nel cyberspazio ossia l'impossibilità di attribuire con sicurezza la responsabilità degli attacchi informatici. Le indagini forensi possono richiedere anche anni e la possibilità di negare in maniera plausibile di aver commesso un'intrusione cibernetica (*plausible deniability*) riduce il rischio di rappresaglie e mina i requisiti alla base della deterrenza, consentendo all'aggressore di continuare a operare in una "zona grigia". Un elemento essenziale per analizzare l'approccio nordcoreano al dominio cibernetico è costituito dal fatto che la maggior parte della popolazione, come anticipato, non ha accesso alla rete Internet globale e in più il paese ha alle spalle il "Great Firewall" cinese. Inoltre, gli unici provider che forniscono accesso alla rete Internet ai nordcoreani sono la cinese Unicom dal 2010 e la russa TransTeleCom.[65] Nel 2017, anno in cui ha preso avvio il servizio russo, TransTeleCom era ritenuta gestire il 60 per cento del traffico Internet della Corea del Nord mentre Unicom il restante 40 per cento.[66]

Detto ciò, il persistente e talvolta sfacciato cyber attivismo nordcoreano ha fornito elementi utili per inquadrare gli attori, le capacità messe in campo e gli obiettivi.[67] Con l'aumento della portata e dei livelli di sofisticatezza delle tattiche, tecniche e procedure le unità informatiche della Corea del Nord si sono specializzate in base alle lezioni apprese attaccando obiettivi diversi adattando continuamente il codice malware per evitare di essere rintracciati. Secondo una recente analisi di McAfee Labs i gruppi sponsorizzati dallo stato nordcoreano "eseguono operazioni informatiche mirate secondo le rispettive competenze e collaborano tra loro per operazioni più complesse ed estese che richiedono una combinazione di competenze e strumenti."[68] Gli analisti delle società di sicurezza informatica che hanno monitorato e studiato gli attacchi informatici passati hanno denominato questi gruppi rintracciati in Cina, Russia, Sudest asiatico, Nord America, Africa ed Europa con vari pseudonimi perlopiù in base al malware e alle tattiche osservate associando, per esempio, APT37 (Reaper), Kimsuky e Sun Team al cyber-spionaggio politico mentre i gruppi Andariel, APT 38 (Bluenoroff), collegati a Lazarus, alle estorsioni finanziarie e criminalità informatica.[69] In particolare, la varietà di strumenti del gruppo

[64] "N.K. establishes university named after leader Kim", *Yonhap*, 14 ottobre 2020.
[65] W. Martyn, "Russia Provides New Internet Connection to North Korea", *38 North*, 1 ottobre 2017.
[66] "Russian firm provides new internet connection to North Korea", *Reuters*, 2 ottobre 2017.
[67] Si veda, ad esempio, l'avviso sulla sicurezza informatica pubblicato congiuntamente dalla Cybersecurity and Infrastructure Security Agency (CISA), dal Federal Bureau of Investigation (FBI) e dalla Cyber National Mission Force (CNMF) degli Stati Uniti sulle tattiche, le tecniche e le procedure utilizzate dal gruppo Kimsuky, https://us-cert.cisa.gov/ncas/alerts/aa20-301a
[68] J. Rosenberg Jay e C. Beek, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families", *McAfee Labs*.
[69] "Lazarus arisen: Architecture, tools, attribution", *Group I-B*, 30 maggio 2017.

Lazarus e la sua determinazione hanno attirato l'attenzione dell'intelligence e delle forze dell'ordine di vari paesi con gli Stati Uniti come capofila nell'ambito degli sforzi del loro *Cyber Command* e del *Department of Homeland Security* per ostacolare le infrastrutture informatiche offensive dei paesi rivali.

L'alleanza Stati Uniti-Corea del Sud alla prova della deterrenza cibernetica

Attacchi come *WannaCry* sono citati per sottolineare che comportamenti informatici sempre più distruttivi stanno innalzando il tasso di rischio di errori di calcolo in situazioni di crisi dovuto alla mancanza di linee rosse condivise nel dominio cibernetico. Nonostante le operazioni informatiche generalmente non siano influenzate dallo spazio fisico, la prossimità geografica nella penisola coreana è un fattore che può mettere in discussione anche gli assunti della sicurezza cibernetica. La politica estera e di difesa nazionale della Corea del Nord, così come il modo in cui Pyongyang utilizza le tecnologie dell'informazione e della comunicazione, sono strettamente legate alle conseguenze della divisione della penisola coreana. Nel caso di una crisi o di un conflitto nella penisola le dinamiche di escalation potrebbero facilmente estendersi ad altri domini. Dall'armistizio del luglio 1953 la Corea del Nord ha continuato con vari gradi di intensità a operare in una "zona grigia" di provocazioni e aggressioni militari circoscritte contro la Corea del Sud attraverso veicoli aerei senza equipaggio, spie infiltrate oltre il confine, sabotaggi aerei, terrorismo, mine lungo la linea demilitarizzata e test nucleari e missilistici. Nonostante ciò, gli Stati Uniti hanno fornito alla Corea del Sud una deterrenza estesa sostenuta dalle armi nucleari che è riuscita a dissuadere Pyongyang in quasi settant'anni dal mettere in atto delle nuove aggressioni su larga scala con effetti sul piano strategico, circostanza che costituisce il *casus foederis* dell'alleanza tra Washington e Seoul.

L'interesse per la guerra cibernetica ha spinto la Corea del Nord durante gli anni Novanta ad attingere ampiamente dall'*electronic intelligence warfare* dell'Esercito di liberazione popolare cinese che a sua volta si è basato sull'osservazione delle operazioni informatiche durante la prima guerra del Golfo e dalle operazioni della Nato nei Balcani.[70] L'aggiunta delle operazioni nel dominio cibernetico al deterrente nucleare e missilistico nordcoreano, che sotto Kim Jong Un ha compiuto rapidi avanzamenti diventando più credibile e integrato, ha aggravato la minaccia asimmetrica di Pyongyang nei confronti della Corea del Sud, delle 28.500 forze armate statunitensi stanziate nel paese e della stabilità regionale nel suo complesso. Tra gli analisti della sicurezza prevale lo scetticismo in merito alla possibilità che Pyongyang possieda la capacità di impegnarsi in una guerra cibernetica sostenuta contro obiettivi militari in uno scontro diretto con gli Stati Uniti e la Corea del Sud.[71] Ad oggi non ha dimostrato la capacità di creare armi cibernetiche fisiche con effetti cinetici. Ciò non toglie che in uno scenario di guerra fisica gli attaccanti nordcoreani possano colpire reti elettriche, dighe, gasdotti e altri sistemi di controllo nell'industria civile e causarne la paralisi tramite DDoS allo scopo di ostacolare la risposta delle forze armate avversarie.[72]

Gli attacchi informatici alle infrastrutture critiche o alle reti militari della Corea del Sud hanno il maggior potenziale per produrre, da soli o in combinazione con armi convenzionali o nucleari, effetti strategici; per questo in Corea del Sud è in fase di sviluppo un quadro per la protezione delle

[70] D. Pinkston, *op. cit*, p. 62.
[71] R.C. Maness, B. Valeriano e B. Jensen, "North Korea's Offensive Cyber Program Might Be Good, But Is it Effective?", *Council for Foreign Relations*, 25 ottobre 2017.
[72] U.S. Department of the Army, "North Korean Tacticss", Army Techniques Publication (ATP) 7-100 series, luglio 2020.

infrastrutture nazionali critiche e dei sistemi operativi militari.[73] L'hackeraggio della *Korea Hydro and Nuclear Power* nel 2014 e del Ministero della difesa due anni dopo esemplifica la tipologia di attacchi che l'alleanza dovrebbe contrastare mentre a Seoul spetterebbe la responsabilità di scoraggiare, difendere e rispondere agli attacchi di livello inferiore come quelli ai siti Web del governo, delle società finanziarie e dei media. Nel giugno 2021 il *Korea Atomic Energy Research Institute*, un istituto di ricerca finanziato dal governo e incaricato di sviluppare la tecnologia nucleare ha ammesso che 13 indirizzi IP esterni hanno violato la rete interna utilizzando l'indirizzo e-mail di Moon Chung-in, l'ex consigliere speciale per la politica estera del presidente sudcoreano Moon Jae-in, e almeno un indirizzo sarebbe riconducibile al gruppo di hacker nordcoreano Kimsuky.[74] Con obiettivi che vanno dai governi alle banche ai media, gli attaccanti nordcoreani rappresentano una minaccia cibernetica peculiare. Nel 2011 il Ministero della difesa della Corea del Sud ha lanciato il Piano generale di sicurezza cibernetica al fine integrare tutte le capacità militari nazionali contro le minacce informatiche. Nell'aprile 2019 la Casa Blu ha pubblicato la Strategia nazionale per la sicurezza informatica che menziona la deterrenza senza specificare alcun particolare attaccante informatico, presumibilmente per salvaguardare l'approccio distensivo promosso dal presidente Moon verso la Corea del Nord. L'elaborazione della deterrenza informatica sudcoreana che emerge da questi documenti è ascrivibile alla "deterrenza per negazione" e a differenza dei recenti documenti sulla strategia di sicurezza informatica degli Stati Uniti non vi è alcuna menzione esplicita dell'utilizzo di tutti gli strumenti del potere nazionale (*whole-of-government approach*) per stabilire una "deterrenza per punizione".[75]

Le capacità informatiche della Corea del Sud si sono evolute nel quadro strategico dell'alleanza. A questo proposito si ritiene che le forze congiunte non abbiano ancora innalzato il loro potenziale tecnologico-militare al livello d'innovazione organizzativa, concettuale e operativa necessaria per utilizzare le tecnologie avanzate in modi nuovi avendo così concesso alla Corea del Nord un relativo margine di vantaggio per combinare il suo programma nucleare e missilistico con capacità informatiche che offrano al regime alternative a minor costo per esercitare ulteriore pressione sulla comunità internazionale. Gli alleati hanno rilasciato diverse dichiarazioni congiunte sulla cooperazione nel dominio informatico in cui l'attenzione è posta sulla protezione delle infrastrutture critiche e delle reti militari. [76] Non hanno prodotto invece alcun documento dedicato alla deterrenza informatica nell'ambito dell'alleanza bilaterale, perché, presumibilmente, entrambi i paesi stanno ancora sviluppando le proprie strategie, politiche e organizzazioni per gestire il dominio cibernetico il che ritarda anche la creazione di un'efficace posizione comune. Anche gli Stati Uniti e il Giappone hanno concordato che il loro Trattato di reciproca sicurezza includerà i gravi attacchi informatici contro entrambi i paesi, in linea con il dibattito internazionale in corso sui pesanti rischi per la sicurezza di ciascuno stato. La comunità internazionale ha iniziato a discutere l'ipotesi che gli attacchi informatici possano attivare l'autodifesa o la difesa collettiva. Per quanto riguarda la Nato, ad esempio, la difesa informatica cooperativa è stata avviata a seguito dell'attacco informatico all'Estonia nel 2007 e il Manuale di Tallinn, che tenta di applicare il diritto internazionale alle operazioni informatiche, sostiene l'applicazione dell'autodifesa e della difesa collettiva agli attacchi informatici. Ritornando all'Asia orientale, Washington e i suoi due alleati storici devono affrontare dilemmi molto simili a quelli descritti precedentemente per il dominio marittimo, a partire dalla mancanza di un quadro giuridico

[73] Ministry of Defense of the Republic of Korea, "2020 Defense White Paper", 2020.
[74] "N.K. hacking group breached S. Korean nuclear research institute last month: lawmaker", *Yonhap*, 18 giugno 2021.
[75] J.E. Platte, "Defending Forward on the Korean Peninsula", *The Cyber Defense Review*, vol. 5, n. 1, pp. 84-85.
[76] The White House, "Joint Fact Sheet: The United States-Republic of Korea Alliance: Shared Values, New Frontiers", 16 ottobre 2015.

per affrontare gli attacchi informatici e le questioni relative alle contromisure che riesca a livellare e rendere omogenee tra questi paesi le rispettive soglie di attivazione dell'autodifesa e della difesa collettiva. Peculiare del dominio cibernetico è invece l'impossibilità di misurare l'entità dell'attacco e dei danni subiti per stabilire una "linea rossa" che giustifichi l'autodifesa a causa del fatto che le operazioni informatiche possono essere condotte in remoto anche da singoli attaccanti e che la capacità di rilevamento e attribuzione è stata finora insufficiente per rimuovere qualsiasi ombra di dubbio. Nel complesso, queste operazioni sono al di sotto della soglia che giustificherebbe altrimenti una risposta collettiva secondo le clausole previste dai trattati bilaterali che compongono il sistema di alleanze cosiddetto "*hub-and-spoke*", portano alla luce le difficoltà di coordinamento a livello bilaterale, derivanti soprattutto dalle percezioni difformi circa l'origine delle minacce e i diversi vincoli all'uso della forza (i limiti giapponesi sono notoriamente più rigorosi di quelli a cui è sottoposto l'alleato statunitense), e ancor più a livello trilaterale espressione in larga parte dell'antagonismo storico tra Seoul e Tokyo che negli anni ha ostacolato qualsiasi tentativo di formalizzare un'alleanza a tre. Gli accordi bilaterali sulla sicurezza informatica restano quindi il primo passo, e probabilmente anche l'unico contemplabile nel breve periodo, per promuovere la resilienza e l'interoperabilità all'interno delle alleanze degli Stati Uniti con il Giappone e la Corea del Sud per fronteggiare gli attacchi informatici a partire da quelli riconducibili al regime di Kim Jong Un.

Il fattore Covid-19

É opinione condivisa dalla maggior parte degli osservatori internazionali che dopo diciotto mesi gli effetti delle misure per impedire il diffondersi della pandemia da Covid-19 in Corea del Nord siano comparabili, se non superiori, a quelli di decenni di sanzioni internazionali nel mettere in ginocchio la sua economia. Tra marzo e aprile 2021 si sono susseguite voci sulla possibile e parziale riapertura delle frontiere nordcoreane, ma sono bastate poche settimane per metterle effettivamente a tacere. Durante il plenum del Partito a inizio giugno niente ha lasciato supporre che il regime sia disposto a fare un passo indietro e allentare le restrizioni draconiane al commercio con l'estero mentre fuori imperversa ancora il virus che ha assunto tutti i tratti di una "minaccia esistenziale" per la leadership nordcoreana. Se le costanti dichiarazioni circa l'assenza di casi registrati di nuovo coronavirus in Corea del Nord restano difficili da credere, le misure anti-contagio stanno avendo conseguenze drammatiche sulla produzione alimentare esacerbate dalle conseguenze delle inondazioni dell'estate 2020 e dall'assenza di organizzazioni umanitarie internazionali sul campo. L'isolamento autoimposto per sigillare il paese ha privato il regime di cospicue fonti di valuta estera a partire da quelle lecite provenienti dal turismo, uno dei pochissimi settori esclusi dalle sanzioni internazionali. Il 90 per cento del turismo in Corea del Nord proviene dalla Cina e per questo è stato interrotto già il 21 gennaio 2020. Sette giorni dopo, Pyongyang ha chiuso ufficialmente tutti i confini e lo shock è stato immediato. La dipendenza commerciale dalla Cina (quasi il 92 per cento) e dalla Russia ha prodotto l'impennata dei prezzi di alcuni beni primari registrata nella capitale nordcoreana. Secondo i dati doganali di Pechino, da cui naturalmente sono esclusi gli scambi non ufficiali, le esportazioni nordcoreane verso la Cina sono calate nel primo quadrimestre del 2020 del 96 per cento mentre le importazioni sono scese di oltre il 50 per cento nello stesso periodo. All'inizio di quest'anno l'export nordcoreano ha registrato livelli quasi pari a zero ad eccezione di 3,2 milioni di dollari di energia idroelettrica sempre diretta in Cina.[77]

[77] General Administration of Customs of the PRC, http://www.customs.gov.cn/customs/302249/302274/302277/302276/3017299/index.html

Il plenum dello scorso giugno è stato l'ultimo di una serie di eventi pubblici nel corso degli ultimi due anni in cui Kim ha ammesso un certo grado di fallimento (confermando in questo un approccio tattico e politico alla leadership diverso rispetto a quello paterno) nella gestione economica senza per questo attribuirsi direttamente la responsabilità. Difficilmente la Corea del Nord potrebbe tornare a una reale centralizzazione dell'economia – il sistema pubblico di distribuzione è collassato da quasi trent'anni – ma il timore è che le deboli forze di mercato finora tollerate e mai legittimate saranno schiacciate da azioni predatorie determinate dalla necessità del regime di riaffermare la sua presa sull'amministrazione delle risorse economiche per compensare le enormi perdite subite.

In assenza di stime, anche approssimative, sull'aumento dell'evasione delle sanzioni imposte alla Corea del Nord tramite strumenti online durante la pandemia, rispetto agli illeciti condotti mediante scambi via terra e nave, è presumibile che il Covid-19 abbia ulteriormente facilitato il crimine informatico incluso quello sponsorizzato dallo stato nordcoreano, innanzitutto per il semplice fatto di aver rafforzato la tendenza di un sempre maggior numero di istituzioni, servizi finanziari e individui che conduce le proprie attività online e ricorre con più frequenza alle transazioni virtuali e alle valute digitali. Gli esperti dell'Onu incaricati di verificare l'applicazione delle risoluzioni del Consiglio di Sicurezza hanno documentato nel loro ultimo rapporto il perdurare degli illeciti informatici attribuibili al regime nordcoreano durante il periodo di riferimento, dal 4 agosto 2020 al 5 febbraio 2021, volti a ottenere risorse finanziarie virtuali e moneta *fiat* (a corso legale) nonché attacchi informatici contro gli stessi funzionari degli Stati membri.[78] Parallelamente all'hackeraggio di aziende farmaceutiche e l'infiltrazione nelle catene di approvvigionamento dei vaccini, gli esperti di sicurezza informatica segnalano che dall'inizio della pandemia la Corea del Nord potrebbe aver intensificato le sue attività informatiche attraverso i social media, presumibilmente, sfruttando la "minor attenzione" dei lavoratori da remoto alla salvaguardia della sicurezza informatica sulle piattaforme quali Facebook, Twitter e LinkedIn.[79] Nel 2020, ad esempio, il gruppo Lazarus, uno dei gruppi su cui negli anni si sono concentrate in modo specifico le investigazioni internazionali, avrebbe intensificato una strategia definita "honeypot", già osservata nei tre anni precedenti, nei confronti di società europee e israeliane nei settori della difesa, dell'aviazione e dell'energia sfruttando il social network professionale LinkedIn come vettore per l'attacco grazie alla sua reputazione e alla facilità nella raccolta di informazioni sul profilo professionale della vittima. Inviando un'offerta di "lavoro da sogno" per conto di alcune delle più importanti società di difesa e aerospaziale negli Stati Uniti, tra cui Boeing, Lockheed Martin e BAE, gli attaccanti hanno stabilito una relazione personale coi potenziali target con messaggi privati dall'apparenza innocui a cui hanno poi recapitato e-mail contenenti malware.[80]

Le cyber sanzioni europee

La posizione ufficiale dell'Unione europea (Ue) in riferimento alla Corea del Nord si è strutturata per anni lungo due binari paralleli combinando la pressione delle sanzioni indirizzate a colpire le attività di proliferazione del regime col mantenimento di un canale aperto di dialogo e cooperazione. Questo approccio definito ufficialmente "*critical engagement*" ha cercato di isolare la dimensione degli aiuti umanitari dall'andamento dei rapporti sul piano politico e diplomatico. Ma il congelamento del dialogo

[78] UN Panel of Experts (2021), *Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, 4 marzo 2021.
[79] N. Wiesensee, "DPRK hackers create fake Linkedin accounts so good that even experts are fooled", *NK Pro*, 29 aprile 2021.
[80] ClearSky Cyber Security, "Operation 'Dream Job' Widespread North Korean Espionage Campaign", *Blog*, 13 agosto, 2020.

Ue-Corea del Nord dal 2015 e il blocco quasi totale degli aiuti umanitari al paese, che in passato erano sopravvissuti anche ai momenti di crisi più acuti, hanno contribuito a sbilanciare la posizione europea sul lato delle sanzioni che sono diventate lo strumento principale per orientare il rapporto dell'Ue con Pyongyang. In questo Bruxelles si è allineata alla posizione prevalente nella comunità internazionale. Tra luglio 2020 e marzo 2021 il panorama delle sanzioni autonome imposte dall'Ue nei confronti della Corea del Nord si è allargato fino a includere le violazioni sia della sicurezza cibernetica sia dei diritti umani, queste ultime nel quadro del cosiddetto "Magnitsky Act" europeo, in aggiunta alle disposizioni aventi a oggetto le attività e gli individui connessi al programma di armi di distruzione di massa.[81] Le prime "sanzioni informatiche" nella storia dell'Ue, rivolte anche a gruppi russi e cinesi, fanno parte della "cassetta degli strumenti diplomatici informatici" di cui l'UE si è dotata nel 2017 e che riflette peraltro la stessa logica dell'approccio storico nei confronti della Corea del Nord: la centralità della diplomazia e dei negoziati per affrontare le controversie, in questo caso nel ciberspazio, affiancata allo strumento sanzionatorio per rispondere agli attacchi. Bruxelles ha definito la società Chosun Expo "responsabile di aver fornito assistenza, dall'esterno del paese, agli hacker sponsorizzati da Pyongyang negli attacchi contro l'Autorità di vigilanza finanziaria polacca, la Sony Pictures Entertainment e la Banca centrale del Bangladesh", tuttavia, è improbabile che possa ottenere qualche risultato se consideriamo che altre investigazioni internazionali su Chosun Expo hanno concluso che si tratti di una società di facciata già smantellata. A prescindere dal successo del caso di specie e dal fatto che le sanzioni non equivalgono a un'attribuzione ufficiale degli attacchi ai governi dietro a questi gruppi, si sono poste le basi per futuri interventi da parte di Bruxelles nei confronti del cyber attivismo nordcoreano. Dalla decisione si apprende che l'Ue potrà colpire anche i "facilitatori" di un attacco informatico ed elaborare misure per rispondere ad attacchi non necessariamente contro entità e individui entro i confini dell'Ue qualora le violazioni incidano, e qui il linguaggio è vago, sugli "obiettivi di politica estera e di sicurezza comuni secondo l'articolo 21 del Trattato sull'Unione europea".[82] Con l'approvazione delle successive misure restrittive per abusi sui diritti umani in Corea del Nord – la prima volta che l'Ue ha fatto il nome di alcuni funzionari del regime nordcoreano – la pressione ha assunto un ruolo molto più accentuato rispetto al passato. Gli incentivi positivi che ufficialmente fanno parte dell'approccio complessivo dell'Ue per indurre il regime nordcoreano a rivedere i suoi obiettivi, sembrano essere destinati nel breve e medio periodo a restare un'opzione solo sulla carta.

CONCLUSIONI

Dopo quattro anni di sistematico indebolimento delle istituzioni multilaterali e delle strutture a sostegno della prosperità regionale, l'amministrazione statunitense è tornata a una pratica diplomatica tradizionale e prevedibile nei confronti dei partner e degli alleati. Se il presidente Biden concepisce le alleanze come delle risorse laddove il suo predecessore le aveva svilite considerandole pressoché unicamente come un onere per le finanze statunitensi, il banco di prova per la sua amministrazione è rappresentato dal modo con cui esse saranno collocate all'interno della strategia complessiva degli Stati

[81] Nel marzo 2021 ha trovato applicazione per la prima volta lo EU Global Human Rights Sanctions Regime, un nuovo strumento approvato dal Consiglio dell'Ue il 7 dicembre 2020 che consente all'Ue di applicare misure restrittive nei confronti di singoli individui, entità e organizzazioni, statali e non, responsabili, coinvolti o legati a gravi violazioni dei diritti fondamentali ovunque nel mondo. Lo EU Global Human Rights Sanctions Regime è stato modellato sul cosiddetto Magnitsky Act, una legge che il Congresso statunitense ha adottato nel 2012, e ampliato quattro anni dopo (Global Magnitsky Human Rights Accountability Act), in omaggio a Sergej Magnistky, un avvocato per i diritti umani morto misteriosamente nelle carceri russe nel 2009.

[82] Consiglio dell'Unione europea, Decisione (PESC) 2020/1127, 30 luglio 2020.

Uniti per l'Asia, rispetto alla quale, Washington continuerà ad attendere dai partner un contributo significativo. Nel team del presidente Biden figura un nutrito gruppo di specialisti dell'Asia-Pacifico, a riprova della centralità del quadrante asiatico. Diverse posizioni apicali sono poi occupate da esperti di tecnologia e sicurezza informatica, per esempio, all'interno del Consiglio per la sicurezza nazionale. Queste nomine segnalano la priorità assegnata dall'attuale amministrazione al rafforzamento della collaborazione tra le cosiddette "tecno-democrazie", tra cui spiccano il Giappone e la Corea del Sud, al fine di rinnovare la *governance* internazionale del dominio cibernetico e rafforzare la sicurezza informatica.

Negli ultimi anni la resilienza cibernetica delle reti nazionali si è imposta al centro dei dibattiti nazionali accanto alla necessità di potenziare le capacità di difesa. Un'urgenza determinata da un panorama di attaccanti informatici che si è progressivamente diversificato. Accanto alle sfide provenienti dalla Russia e dalla Cina, considerate come le fonti principali degli attacchi cibernetici, sono cresciute rapidamente le attività offensive ricondotte a Pyongyang. Molti elementi concorrono al successo degli attacchi sponsorizzati dalla Corea del Nord a partire dalla vulnerabilità dei sistemi di sicurezza delle istituzioni finanziarie prese di mira che spesso sono reticenti a notificare le violazioni subite alle proprie reti informatiche. Nel perseguire le sue attività vietate o illegali, la Corea del Nord collabora o sfrutta paesi nei quali il sistema di controllo finanziario sulle esportazioni e la proliferazione è debole. Questo è un elemento a cui si fa solitamente riferimento per sostenere la tesi dell'inefficacia delle sanzioni internazionali contro la Corea del Nord e che riguarda anche le azioni di Pyongyang nella "zona grigia" dello spazio cibernetico. Le unità informatiche nordcoreane si avvalgono, infatti, di gruppi di attaccanti che operano da altri paesi e che, a differenza della maggior parte dei criminali informatici, sono sostenuti dalle risorse di un regime noto per la sua capacità di trarre risorse finanziarie da varie attività illecite – dalla produzione e dal commercio di stupefacenti al contrabbando di avorio e alla contraffazione – per reinvestirle nel programma nucleare e missilistico. La dispersione geografica degli attaccanti al servizio del regime alimenta il dilemma dell'attribuzione, tipico degli attacchi condotti in circostanze di "zona grigia", ulteriormente aggravato da un'altra peculiarità del caso nordcoreano: una rete intranet attraverso cui il regime esercita un controllo capillare sulla diffusione delle informazioni nel paese e permette l'accesso alla rete Internet globale solamente a un gruppo molto ristretto di cittadini. In questo modo, Pyongyang protegge la propria infrastruttura critica da potenziali rappresaglie mentre gli unici provider che forniscono accesso alla rete Internet sono russi e cinesi.

In base alle lezioni apprese attaccando obiettivi diversi e adattando continuamente il codice malware per evitare di essere rintracciati, le unità informatiche della Corea del Nord hanno affinato la portata e i livelli di sofisticatezza delle tecniche e delle procedure. L'evoluzione del *modus operandi* degli attacchi informatici attribuiti ai nordcoreani segnala anche una certa propensione all'escalation nel dominio cibernetico, pertanto, per Seoul è prioritario accelerare il processo di messa in sicurezza delle proprie infrastrutture critiche civili e militari e collaborare con Washington al fine di incorporare il dominio cibernetico nella postura di deterrenza strategica complessiva della loro alleanza bilaterale.

La stessa sfida è stata raccolta dall'alleanza bilaterale che gli Stati Uniti condividono con il Giappone. In questo caso, però, le difficoltà in termini di risposta comune alle sfide nella "zona grigia" emergono prima di tutto sul fronte della sicurezza marittima a causa dei continui tentativi cinesi di erodere la sovranità territoriale giapponese. La controversia tra Tokyo e Pechino nel Mar Cinese Orientale è guidata in larga parte dal risentimento per questioni storiche irrisolte – cardine del nazionalismo cinese supportato da Xi – e da un elevato grado di sfiducia reciproca. Questi elementi, uniti al fatto che il teatro in cui operano le rispettive guardie costiere e forze militari è molto limitato, mantengono costante il rischio di incidenti e di escalation involontarie. Il Pcc sembra intenzionato a procedere con la

presenza delle navi e degli aerei cinesi all'interno del territorio amministrato dal Giappone e lo fa in modi che sfidano la giurisdizione giapponese, ma che restano al di sotto della soglia che farebbe altrimenti scattare una risposta militare. La strategia si regge inoltre su un'asimmetria di fondo: tutte e tre le principali forze marittime cinesi rimangono concentrate prima di tutto nei mari vicini alla Cina. La milizia marittima non è nota per operare al di fuori del Mar Giallo, del Mar Cinese Orientale e del Mar Cinese Meridionale. La Guardia costiera cinese ha a disposizione navi in grado di svolgere operazioni su scala globale, ma il fulcro della sua flotta è dislocato a livello regionale e la stessa Marina dell'Epl, che opera in varie aree del mondo, in uno scenario di conflitto riceverebbe l'ordine di convergere a differenza di quella statunitense. Il fatto che molti stati nella regione stiano rispondendo all'espansione della Guardia costiera cinese potenziando le proprie, introduce delle dinamiche inedite che richiedono un'architettura di comando e controllo molto più efficiente tra gli attori marittimi, governativi e civili, sia a terra sia in mare. A questo proposito, da più parti si sottolinea che uno dei passaggi imprescindibili debba essere il rafforzamento dei programmi di esercitazioni congiunte su base routinaria per migliorare l'interoperabilità tra la guardia costiera e i comandi navali. Affinché i risultati aiutino gli strateghi militari a includere nelle loro considerazioni il crescente ruolo degli attori e delle risorse paramilitari, le simulazioni dovranno prevedere più contingenze in cui l'escalation scaturisca da azioni nella "zona grigia" e coinvolgere attori formalmente non militari come le milizie marittime e i pescherecci.

La Corea del Nord e la Cina hanno impiegato, come messo in luce anche da questo approfondimento, alcune delle tattiche storicamente più frequenti nell'ambito della "zona grigia": presentare un quadro mutato all'avversario ponendolo di fronte alla scelta se rispondere in modo coercitivo o se accettare i nuovi sviluppi, eludere le sue linee rosse che innescherebbero un'escalation con costi elevati e conseguenze imprevedibili e fare ricorso ad attori intermediari spesso non statali. I due casi studio sono esemplificativi specialmente dell'ambiguità circa la natura dello scontro e l'incertezza del quadro legislativo e politico pertinente nei mari e nello spazio cibernetico, ulteriormente acuita dal frequente ricorso ad attori non statali e a risorse paramilitari e civili. Per questo la formulazione delle risposte alle sfide della "zona grigia" richiede innanzitutto una prospettiva di lungo periodo e un approccio che mobiliti tutti gli strumenti a disposizione dei governi e incentivi il coordinamento tra la componente civile e quella militare.

Osservatorio di Politica internazionale

Un progetto di collaborazione
tra Senato della Repubblica, Camera dei Deputati
e Ministero degli Affari Esteri e della Cooperazione Internazionale
con autorevoli contributi scientifici.

L'Osservatorio realizza:

Rapporti
Analisi di scenario, a cadenza annuale, su temi di rilievo strategico per le relazioni internazionali

Focus
Rassegne trimestrali di monitoraggio su aree geografiche e tematiche di interesse prioritario per la politica estera italiana

Approfondimenti
Studi monografici su temi complessi dell'attualità internazionale

Note
Brevi schede informative su temi legati all'agenda internazionale

www.parlamento.it/osservatoriointernazionale

Senato della Repubblica

Camera dei Deputati

Ministero degli Affari Esteri
e della Cooperazione
Internazionale

Coordinamento redazionale:

Senato della Repubblica
Servizio Affari internazionali
Tel. 06-67063666
Email: segreteriaaaii@senato.it