La Deterrenza nel XXImo Secolo: Un'Analisi Storica e Teorica

Niccolò Petrelli
Dipartimento di Scienze Politiche
Università Roma Tre

Nel corso degli ultimi anni, la nozione di *deterrenza*, da tempo praticamente scomparsa dal vocabolario della politica internazionale, è riemersa in numerosi documenti strategici e nella prassi di politica estera di numerosi paesi Europei (inclusa l'Italia essendo il concetto menzionato nel Libro Bianco della Difesa 2015), e non.[1] L'obiettivo di questo progetto è quello di comprendere il ruolo che la *deterrenza* potrebbe svolgere negli affari internazionali nel corso del XXImo secolo attraverso uno studio dell'evoluzione storica della sua teoria e della pratica.

Con il termine 'teoria della deterrenza' ci si riferisce in genere ad un corpus di studi accademici che, dopo la Seconda Guerra Mondiale, è arrivato a dominare la letteratura sugli studi di sicurezza negli Stati Uniti ed in Europa occidentale. Circa quella che potrebbe essere chiamata la storiografia o l'evoluzione della teoria della deterrenza, esistono due scuole di pensiero. Da una parte coloro che, sviluppando un'idea originariamente coniata da Robert Jervis, vedono la teoria della deterrenza evolversi attraverso distinte "ondate". Ognuna di queste sarebbe caratterizzata da un particolare framework analitico, interpretazione del processo della deterrenza, e focus sui mezzi della stessa influenzati (principalmente ma non solo) dai problemi strategici più salienti del momento.[2] Dall'altra, una seconda scuola di pensiero sostiene al contrario che tale periodizzazione sottovaluti i significativi elementi di continuità esistenti tra le varie fasi di sviluppo della teoria, e che la letteratura sulla deterrenza possa in gran parte, sino circa ai primi anni 2000, essere classificata come una singola teoria, con circoscritte sub-variazioni. Secondo tale approccio significative discontinuità nella teoria della deterrenza si sono manifestate

---

1 *Libro Bianco per la Sicurezza Internazionale e la Difesa* (Roma: Ministero della Difesa, 2015).

2 Robert Jervis, 'Review Article: Deterrence Theory Revisited', *World Politics* 31/2 (January 1979), 289-324; Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research', *Contemporary Security Policy*, 31/1 (2010), 1-33; Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda', *International Studies Quarterly* 54/3 (September 2010), 705-732. Per quanto riguarda la diffusione di questo approccio si veda ad esempio Dmitry (Dima) Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force', *Security Studies* 26/1 (2016), 157-184.

solo nel momento in cui il focus analitico si è spostato dallo studio della deterrenza fra stati a quello delle relazioni di deterrenza tra attori statali e non-statali.[3]

L'approccio adottato in questa ricerca sintetizza i punti di vista delle due scuole. Infatti, nel fornire una periodizzazione dell'evoluzione della teoria della deterrenza basata sulla nozione di "ondate" successive, parte dall'assunto che, sebbene diverse sotto molti profili differenti, esse possano essere considerate tutte esplorazioni di un'unica teoria. In ciò la ricerca si ispira all'autorevole opinione secondo cui esiste una sola teoria generale della deterrenza, intesa come un insieme coerente di ipotesi logicamente connesse circa il fenomeno, la cui valenza e applicabilità sono eterne e universali. Tale teoria generale espone la natura della deterrenza come concetto, funzione, e processo e spiega gli elementi che influenzano e guidano specifiche strategie di deterrenza.[4]

Nel mettere insieme le parti costitutive della teoria della deterrenza sparse nella letteratura lo scopo di questo elaborato è euristico, il lavoro è in altre parole finalizzato ad illuminare sia eventuali cambiamenti nell'ontologia del fenomeno della deterrenza, così come evidenziati da modifiche analitiche ed epistemologiche nella teoria, sia evoluzioni concettuali intervenute nel tempo.[5]

La comprensione di tali cambiamenti è a sua volta essenziale per la formazione di coloro che hanno compiti e responsabilità inerenti lo sviluppo della politica estera e di sicurezza a livello nazionale. Sotto questo punto di vista, parafrasando Colin Gray, la teoria generale può essere paragonata a un *passepartout* in grado di arricchire concettualmente coloro che sviluppano e attuano la politica estera e di sicurezza, aprendo una porta su una componente essenziale delle interazioni nell'attuale sistema internazionale.[6]

Anticipando le conclusioni, l'analisi dell'evoluzione della letteratura evidenzia una crescente complessità nel fenomeno della deterrenza la cui struttura e modello di funzionamento possono essere assimilati a un *network*; di tale complessità la letteratura

---

[3] Frank C. Zagare, 'Classical Deterrence Theory: A Critical Assessment', *International Interactions*, 21 (1996), 365–87; Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge University Press, 2000); Frank C. Zagare, *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987). Nel suo fondamentale contributo al tema, John Mearsheimer sottolineava infatti come la sua teoria non si applicasse agli attori non-statali. Si veda John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983).

[4] Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); 8; Colin S. Gray, 'Gaining Compliance: The Theory of Deterrence and its Modern Application', *Comparative Strategy*, 29/3 (2010), 278-283.

[5] Alexander L. George & Andrew Bennet, *Case Studies and Theory Development in the Social Sciences* (Cambridge: the MIT Press, 2005).

[6] Si veda l'introduzione in Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2012).

ha dato conto nella sempre più evidente commistione del concetto di deterrenza con quello di *compellenza*.

Il Concetto di Deterrenza: Aree di Consenso e Criteri Analitici

Il primo passo per sviluppare un framework adeguato ad analizzare l'evoluzione della teoria della deterrenza è ricapitolare i principali elementi di consenso all'interno della stessa circa l'oggetto di riferimento al fine di identificare le dimensioni fondamentali di variazione del concetto. Esse verranno quindi impiegate per delineare una serie di criteri tra essi correlati che aiutino a cogliere le principali differenze tra le varie "ondate" della teoria dalla fine degli anni 40 ad oggi.

Esiste un consenso piuttosto ampio circa la definizione di deterrenza come: la manipolazione, da parte di un attore, del calcolo costi/benefici di un avversario/competitore circa una determinata azione. [7] Riducendo i benefici o aumentando i costi potenziali (o entrambi), è possibile far desistere un avversario/competitore dall'intraprendere un'azione considerata dannosa. [8] Concettualmente, la deterrenza è una forma di influenza coercitiva basata principalmente su incentivi negativi; in termini colloquiali potrebbe essere definita come l'arte del ricatto e della generazione della paura.[9] La deterrenza può considerarsi una forma di influenza in quanto non tenta di controllare l'avversario/competitore, ad esempio cercando di eliminare la sua capacità di agire o di stabilire su di esso una qualche forma di controllo fisico. La deterrenza, al contrario, lascia al "bersaglio", l'attore che ne è fatto oggetto, la possibilità di esercitare una scelta, mirando ad influenzarla. In secondo luogo, la deterrenza può considerarsi coercitiva in quanto utilizza prevalentemente minacce, incentivi negativi. La necessità della deterrenza sorge infatti quando un attore si aspetta che il corso d'azione intrapreso da un avversario/competitore possa condurre ad un esito dannoso.[10] Per tale ragione tende ad incentrare il proprio tentativo di influenza sulla minaccia, pur associandola nella maggioranza dei casi a determinati messaggi o incentivi positivi. L'essenza della deterrenza è quindi la generazione nel bersaglio della convinzione che il proprio corso d'azione porterà a un risultato negativo per i propri

[7] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974), 11.
[8] Austin Long *Deterrence Lessons from Six Decades of RAND Research* (Santa Monica: RAND Corporation).
[9] Daniel Ellsberg, *The Theory and Practice of Blackmail* (Santa Monica: RAND Corporation, 1968).
[10] Bernard Brodie, *The Anatomy of Deterrence* (Santa Monica: RAND, 1958), 1-5; si veda anche Olaf Helmer, *Deterrence* (Santa Monica: RAND Corporation, 1957).

interessi o obiettivi. Da ultimo è importante notare che, per quanto radicato in un calcolo razionale, il concetto di deterrenza consta anche di una componente emotiva. Chiunque scelga di sviluppare una strategia di deterrenza non può fondarla solo su elementi tangibili e misurabili da parte del "bersaglio", poiché il suo calcolo non sarà basato esclusivamente su una valutazione di input noti. Al contrario le strategie di deterrenza presuppongono l'introduzione di un elemento imponderabile al fine di generare incertezza, dubbio, in chi è fatto oggetto di minacce, circa come la forza potrebbe essere utilizzata contro di lui e circa l'impatto che potrebbe avere sui suoi interessi. Tale componente della deterrenza ed il suo funzionamento sono stati magistralmente sintetizzati da Schelling nell'espressione: "la minaccia che lascia qualcosa al caso".[11]

La letteratura distingue tra "situazione di deterrenza", in cui un attore è dissuaso dal compiere determinate azioni senza che nessuno abbia deliberatamente tentato di inviare un messaggio di dissuasione, e "strategia di deterrenza", quando tale comportamento fa seguito a un segnale deliberatamente elaborato e inviato.[12] Idealmente, nel momento in cui un attore opta per una "strategia di deterrenza", si procede a sviluppare un programma di deterrenza guidato da un particolare obiettivo politico e fondato su ipotesi di intelligence relative alle intenzioni e capacità dell'avversario e su una stima della correlazione di forze o "net assessment".[13] Teoricamente, nella prima fase di questo programma, i pianificatori della deterrenza delineano la percezione di minaccia dell'avversario/competitore e identificano i "valori" strategici che possono essere effettivamente minacciati e messi a rischio; in una fase successiva, cercano modi e mezzi per sfruttare queste paure nel modo più efficace, al fine di modellare il calcolo strategico dell'avversario. In questa ultima fase, i pianificatori comunicano minacce inequivocabili

[11] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 74. Si veda anche: Robert Jervis, 'The Confrontation between Iraq and the US: Implications for the Theory and Practice of Deterrence', *European Journal of International Relations*, 9/2 (June 2003), 325.

[12] Stephen L. Quackenbush, 'Deterrence theory: Where Do We Stand?', *Review of International Studies*, 37 (2011), 750; Patrick Morgan, 'The Concept of Deterrence and Deterrence Theory', *Oxford Research Encyclopedia of Politics* (Oxford: Oxford UP, 2017) https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-572

[13] Sul net assessment si veda: Philip Karber, Net Assessment *for SecDef. Future Implications from Early Formulations* (Washington DC: Potomac Foundation, 2015); Niccolò Petrelli, *Net Assessment and Grand Strategy: Theory for Practice* (manoscritto non pubblicato).

che segnalano intenzioni e capacità credibili.[14] Ogni strategia di deterrenza consiste in altre parole in tre elementi: capacità; minaccia; comunicazione.[15]

La deterrenza dipende quindi in primo luogo dalla presenza di effettive capacità di mettere in atto la minaccia che si intende comunicare. Tali capacità, di qualsiasi tipo esse siano, devono necessariamente trovarsi in una condizione di "prontezza operativa", ovvero devono poter essere rapidamente impiegate e devono, almeno in una certa misura, essere visibili al soggetto verso cui si indirizza la minaccia deterrente.[16] Per esempio, durante la crisi di Kargil tra India e Pakistan del 1999, il Pakistan attivò le proprie capacità nucleari con il solo scopo di mandare un messaggio a Nuova Delhi. Islamabad era infatti consapevole che gli USA avrebbero monitorato attentamente ogni attività relativa all'arsenale nucleare e sfruttò la circostanza per cercare di "deterrere" l'India.[17] La componente capacitiva della deterrenza ne costituisce la fondamentale base materiale, ovvero l'elemento in grado di condizionare la componente razionale del calcolo strategico dell'avversario.[18]

In secondo luogo, la deterrenza dipende da una percezione di credibilità della minaccia formulata che, come la letteratura ha evidenziato, può divergere, in maniera anche significativa, dalla realtà oggettiva. Essa è infatti in primo luogo influenzata dalla situazione specifica in cui viene comunicata: la minaccia di un attacco nucleare in risposta a una "provocazione" grave è certamente più credibile di una minaccia analoga in risposta a un'aggressione "minore".[19] Esiste tuttavia anche un'altra componente della credibilità,

---

[14] Paul Huth and Bruce Russett, 'Testing Deterrence Theory: Rigor Makes a Difference', *World Politics* 42/4 (July 1990), 466-501; in relazione alla procedura di applicazione del net assessment a seguito della traduzione della deterrenza in una strategia si veda: Williamson Murray, 'Operational Net Assessment Or, Preparing to Lose the Next War', in NIDS International Symposium on Security Affairs, *Strategic Management of Military Capabilities: Seeking Ways to Foster Military Innovation* (Tokyo: National Institute for Defense Studies, 2013), 43-55; Michael J. Hannan, *Operational Net Assessment: A Framework for Social Network Analysis and Requirements for Critical Debate* (Monterey: Naval Postgraduate School, 2005); Emily Mushen and Jonathan Schroden, Are *We Winning? A Brief History of Military Operations Assessment* (Arlington: Center for Naval Analyses, 2014). 9-10.

[15] T.V. Paul, 'Complex Deterrence: An Introduction' in T.V. Paul, Patrick Morgan, and James Wirtz (eds.), *Complex Deterrence* (Chicago: University of Chicago Press, 2009), 3.

[16] William W. Kaufmann, *The Evolution of Deterrence 1945–1958* (Santa Monica: RAND Corporation, 1958), 58.

[17] Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton: Princeton University Press, 2014), capitoli 3 & 4.

[18] Si vedano ad esempio: Brendan Rittenhouse Green & Austin Long, *The Role of Clandestine Capabilities in Deterrence: Theory and Practice* (U.S. Naval Postgraduate School Project on Advanced Systems and Concepts for Countering WMD Final Report September 2017) e Keith B. Payne, 'Maintaining Flexible and Resilient Capabilities for Nuclear Deterrence', *Strategic Studies Quarterly* 5/2 (Summer 2011), 13-29.

[19] Robert Jervis, 'Deterrence and Perception', *International Security* 7/3 (Winter, 1982-1983), 3-30; Richard Ned Lebow and Janice Gross Stein, 'Rational Deterrence Theory: I Think, Therefore I Deter', World Politics 41/2 (January 1989), 208-224; Richard Ned Lebow and Janice Gross Stein, 'Beyond Deterrence'. *Journal of Social Issues* 43/4 (1987), 5-71.

che è inerente al soggetto che formula la minaccia, non alla situazione. In circostanze identiche, la minaccia di un attore può essere credibile laddove quella di un altro non lo sarebbe. In parte, come pocanzi asserito, ciò deriva dalle capacità di attuare la minaccia nonché da quella di difendersi dalla risposta dell'altro. Ma c'è di più; è stato infatti chiaramente dimostrato che la credibilità è legata alla "reputazione", alla percezione di risolutezza rispetto al prezzo da pagare per impedire una determinata azione da parte di un avversario.[20] Ciò spiega in parte come mai tanti — tra cui l'allora Segretario della Difesa Chuck Hagel — abbiano criticato l'amministrazione di Barack Obama quando, dopo aver tracciato linee rosse circa l'uso di armi chimiche in Siria, decise poi di non intervenire per sanzionare il comportamento di Bashar al-Assad.[21] Parimenti, il fatto che dopo la guerra del 2006 tra Israele ed Hezbollah, non vi siano più stati conflitti tra i due attori suggerisce quanto la strategia israeliana abbia avuto dei meriti, come in parte ha poi ammesso lo stesso leader di Hezbollah anni dopo. Hassan Nasrallah infatti, in una intervista concessa qualche tempo dopo la fine della guerra, ha infatti dichiarato che la sua organizzazione non si aspettava una tale reazione da parte di Israele. Reazione che ha certamente contribuito ad evitare scontri diretti da ormai molti anni a questa parte.[22] Il dato è interessante se si pensa che, da un punto di vista di strategia militare e operativo, Israele uscì perdente da quella guerra il cui valore, assumendo che la nostra interpretazione sia corretta, può dunque essere compreso solo nel medio-lungo termine.[23]

La deterrenza consiste in una richiesta nei confronti di un altro attore di astenersi dal fare qualcosa, ed è una relazione iterativa che richiede significative capacità di comunicazione. L'attore che intende esercitare deterrenza deve far sì che l'avversario che intende scoraggiare da un certo corso d'azione comprenda chiaramente i contorni della

[20] Bruce H. Clark and David B. Montgomery, 'Deterrence, Reputations, and Competitive Cognition', *Management Science* 44/1 (January 1998), 62-82.
[21] Hal Brands, American Grand Strategy in the Age of Trump (Washington DC: Brookings Institution Press, 2018), capitoli 2 & 3.
[22] Daniel Sobelman, 'Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–16', *International Security* 41/3 (Winter 2016/17), 151-196.
[23] Daniel Byman, "An Eye for a Tooth: Israel's problem with deterrence," Foreign Policy, July 24, 2014. Per quanta riguarda il fallimento operative e strategico-militare, si veda Uri Bar-Joseph, "Israel's Military Intelligence Performance in the Second Lebanon War," *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 3 (2007), pp. 583-601. Per quanto riguarda il successo militare e i suoi differenti piani, si veda Allan R. Millett, Williamson Murray, and Kenneth H. Watman, "The Effectiveness of Military Organizations," in Allan R. Millet and Williamson Murray, *Military Effectiveness: Volume 1: The First World War* (Cambridge: Cambridge University Press, 2010, New Edition), 1-30.

minaccia.[24] Fare in modo che un avversario/competitore comprenda il messaggio deterrente attraverso "il frastuono e il rumore" della politica internazionale richiede significativi sforzi pubblici e privati di comunicazione.[25] E' utile precisare che con l'espressione "chiarezza di comunicazione" si intende chiarezza rispetto all'evento o azione che si vuole evitare, le cosiddette "linee rosse", ma non necessariamente si implica chiarezza rispetto alla minaccia. La politica statunitense e, per estensione quella della NATO, durante la Guerra fredda è un ottimo esempio: qualunque tentativo di invadere la Germania dell'Ovest da parte Sovietica avrebbe portato ad una immediata e spropositata reazione.[26] Le minacce di deterrenza possono però anche essere (e spesso sono deliberatamente) ambigue per numerose ragioni, inclusa la convinzione che una minaccia troppo specifica possa rivelarsi controproducente in alcune circostanze o rispetto ad alcune categorie di attori.[27]

Da questa descrizione del consenso accademico e professionale circa la natura della deterrenza discende il nostro argomento generale secondo cui è possibile identificare quattro dimensioni fondamentali di variazione del concetto:

- Attori;
- Capacità;
- Meccanismo;
- Processo.

La prima dimensione si riferisce al numero di attori il cui calcolo la strategia di deterrenza adottata intende influenzare. Come nella teoria dei giochi, il numero degli attori coinvolti nella relazione di deterrenza incide in maniera significativa sulle dinamiche di interazione tra gli stessi.[28] La seconda dimensione riguarda il tipo di capacità impiegate nel tentativo di far desistere uno o più avversari/competitori da una determinata azione, capacità che possono variare tra "cinetiche" e "non-cinetiche". Il terzo criterio di variazione riguarda il

---

[24] Jack S. Levy, 'When Do Deterrent Threats Work?', *British Journal of Political Science* 18/4 (October 1988), 486.

[25] James M. Acton, 'Extended Deterrence and Communicating Resolve' *Strategic Insights*, 8/5 (December 2009); Michael Gerson & Daniel Whiteneck, *Deterrence and Influence: The Navy's Role in Preventing War* (Arlington: Center for Naval Analyses, 2009); Michael McCanles, 'Machiavelli and the Paradoxes of Deterrence', Diacritics 14/2 (Summer 1984), 11-19.

[26] David N. Schwartz, 'The Role of Deterrence in NATO Defense Strategy: Implications for Doctrine and Posture', *World Politics* 28/1 (Oct., 1975), 118-133; David S. Yost, 'Assurance and US Extended Deterrence in NATO', *International Affairs* 85/4 (Jul., 2009), 755-780.

[27] Steven Pifer, 'Dealing with Russia and Drawing Red Lines', *Order from Chaos Blog*, March, 10, 2017 https://www.brookings.edu/blog/order-from-chaos/2017/03/10/dealing-with-russia-and-drawing-red-lines/; Yoel Guzansky, 'Lines in the Sand: the Use and Misuse of Red Lines', *Defense & Security Analysis* 31/2 (2015), 90-98.

[28] Prajit K. Dutta, *Strategies and Games: Theory and Practice* (Cambridge: The MIT Press, 1999).

"meccanismo" di funzionamento della deterrenza, dunque fondamentalmente il tipo di minaccia che si formula nei confronti di un avversario o competitore. L'ultima dimensione di variazione concerne invece la prevalenza della componente *fisica* o *psicologica* nel processo attraverso cui il meccanismo dispiega il suo effetto.
Tali dimensioni verranno utilizzate come criteri per analizzare i cambiamenti nel fenomeno e nel concetto della deterrenza attraverso le varie ondate di ricerca.

Le Prime Tre Ondate: 1945-1990

La prima ondata di teorizzazione sulla deterrenza emerse all'indomani della Seconda Guerra Mondiale ispirata dalla necessità di riflettere sulle implicazioni per la politica internazionale e la strategia, in primo luogo, dell'invenzione della bomba atomica, in secondo luogo della guerra fredda tra USA e URSS.[29] Bernard Brodie, Arnold Wolfers e Jacob Viner possono essere considerati le figure più rilevanti di tale fase iniziale di riflessione sulla deterrenza. In particolare Bernard Brodie fu probabilmente il primo a rendersi conto che il sistema internazionale del secondo dopoguerra era radicalmente diverso dal sistema multipolare europeo che lo aveva preceduto, sostanzialmente ancora modellato su quello Bismarkiano. [30] Appariva dunque necessario sviluppare un framework teorico di analisi in grado di illuminare le nuove realtà strategiche emerse dal conflitto: la moderna teoria della deterrenza, nelle sue iniziali formulazioni una ricalibrazione della teoria classica dell'equilibrio di potere, rappresentò tale framework.[31]

Facendo uso di concetti ed idee originariamente sviluppati nel periodo precedente la Seconda Guerra Mondiale, e legati al maturare del potere aereo, la prima ondata di teoria si concentrò dunque su un contesto bipolare in cui gli attori coinvolti nella relazione di deterrenza erano dotati di armi atomiche e poi termonucleari.[32] Il meccanismo attraverso cui si riteneva che strategie di deterrenza potessero funzionare era quello della

[29] Friedrich Kratochwil, *International Order and Foreign Policy* (Boulder: Westview Press, 1978), 155-156.
[30] Bernard Brodie (Ed.) *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946).
[31] John Raser, 'Deterrence Research: Past Progress and Future Needs', *Journal of Peace Research* 3/4 (1966), 297-327.
[32] George H. Quester, *Deterrence before Hiroshima. The Airpower Background of Modern Strategy* (New York: John Wiley & Sons, 1966), 2; R.J. Overy, 'Air Power and the Origins of Deterrence Theory before 1939', *Journal of Strategic Studies* 15/1 (1992), 74-76; Richard Mueller, 'The Origins of Mad: A Short History of City-Busting', in Henry D. Sokolski (ed.) *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice* (Carlisle: Strategic Studies Institute, US Army War College 2004), 32. La differenza è che un'arma atomica sfrutta la fissione nucleare, che divide un atomo più grande in due più piccoli, per generare energia. Un'arma termonucleare, anche detta all'idrogeno, si basa invece sulla fusione di due o più atomi in uno più grande e genera una potenza molto maggiore.

"punizione" (*by punishment*). La deterrenza "per punizione" non si focalizzava su una qualche forma di rappresaglia a difesa diretta dell'obiettivo minacciato dall'avversario, ma piuttosto sulla minaccia di una punizione più ampia, potenzialmente anche non collegata al contesto operativo del confronto, la cui conseguenza era di aumentare in maniera significativa il costo dell'attacco. Punire un avversario equivaleva ad infliggergli un livello di "dolore" (o "costo", nella formulazione di Thomas Schelling) sproporzionato rispetto al potenziale guadagno. In sostanza il meccanismo della "punizione" si concretizzava della minaccia di colpire la popolazione civile di un avversario/competitore anche senza averlo attaccato militarmente prima.[33]

Un'ultima caratteristica della prima ondata di teoria della deterrenza è quella di concettualizzare il processo della deterrenza come prettamente psicologico ed estremamente rapido, quasi istantaneo. Poiché la logica della deterrenza era fondata sulla minaccia di un danno "spropositato", attraverso una capacità militare "straordinaria" (l'arma atomica e poi termonucleare), si tendeva a concepire il processo della stessa come implicante principalmente la generazione di effetti cognitivi, più che fisici, nel soggetto che si intendeva dissuadere.[34]

La seconda ondata di teoria della deterrenza prese piede intorno alla metà degli anni 50 per concludersi all'incirca verso la fine degli anni 60, quando le metodologie ed i modelli analitici impiegati (derivati principalmente dalla teoria dei giochi e dalla "analisi dei sistemi" sviluppata alla RAND Corporation) caddero in disgrazia per via della evidente inadeguatezza a guidare le decisioni strategiche americane in Vietnam.[35] Il tentativo di "misurare" quantitativamente gli effetti fisici e psicologici generati dalle operazioni militari in Indocina, per quanto accurato, generava infatti una tipologia di dati sostanzialmente inutilizzabili come input per decisioni strategiche.[36] Nonostante sia stata oggetto di aspre critiche per la sua natura altamente astratta, la mancanza pressocché totale di senso politico e storico, la seconda ondata produsse importanti contributi teorici, seppur per diverso tempo empiricamente non convalidati.[37]

---

[33] George H. Quester, *Deterrence before Hiroshima,* 3; R.J. Overy, 'Air Power and the Origins of Deterrence Theory before 1939', 80-81, 84.

[34] Barry Steiner, *Bernard Brodie and the Foundation of American Nuclear Strategy* (Lawrence: University Press of Kansas, 1991), 12-15; Paul Huth, 'Deterrence and International Conflict: Empirical Findings and Theoretical Debates', *Annual Review of Political Science*, 2 (1999), 25-48.

[35] Bernard Brodie, 'Why Were We So (Strategically) Wrong?', *Foreign Policy* No. 5 (Winter, 1971-1972), 151-161; Colin S. Gray, 'What Rand Hath Wrought', *Foreign Policy* No. 4 (Autumn, 1971), 111-129.

[36] William S. Murray, 'A Will to Measure', *Parameters* 31/3 (Autumn 2001), 134-147.

[37] Emanuel Adler, 'The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control', *International Organization* 46/1 (1992), 107; Marc Trachtenberg, *History and Strategy* (Princeton: Princeton University Press, 1991), 44-46.

In linea generale, la seconda ondata rimane concentrata principalmente su relazioni di tipo diadico e, allo stesso modo, continua a focalizzarsi sulle capacità nucleari. Appaiono tuttavia anche studi relativi alla deterrenza estesa e convenzionale che contribuirono a sviluppi concettuali importanti, relativi in particolar modo ai meccanismi e al processo della deterrenza.[38] In importanti studi del 1960-61, Glenn Snyder identificò, accanto al meccanismo per così dire "tradizionale" della deterrenza, la "punizione", la deterrenza attraverso "negazione" (*by denial*). Tale meccanismo si basa sulla possibilità di *negare* all'avversario/competitore il vantaggio derivante dall'azione che si accinge ad intraprendere (e che si vuole dissuadere) o, più semplicemente, di rendere fisicamente difficile per esso compierla.[39] Gli studiosi della seconda ondata evidenziarono come l'attivazione di questo meccanismo di deterrenza richiedesse, in primo luogo, la capacità di rendere un obiettivo materialmente più difficile da raggiungere ed in secondo luogo, l'abilità di "segnalare", ovvero rendere nota al soggetto recettore, la propria capacità di "interferenza".[40] Esempio classico di deterrenza attraverso "negazione" potrebbe essere considerata la politica britannica del XVIIImo secolo di fornire armamenti agli stati più piccoli d'Europa per scoraggiare aggressioni da parte dei rivali continentali.[41] Anche le forme di deterrenza basate su questo meccanismo prospettano dunque all'avversario/competitore un aumento del costo potenziale di un corso d'azione. Nella deterrenza per "negazione" tuttavia tali costi verranno inflitti durante l'atto stesso di aggressione, nel luogo e nel momento in cui essa si verificherà.

Per quanto riguarda il processo della deterrenza, la seconda ondata non si discosta in maniera significativa dalla visione psicologica della prima ondata; sviluppa tuttavia due aspetti precedentemente ignorati: ovvero la questione della credibilità ed il problema dell'*escalation*. Lo spostamento del focus dalle capacità nucleari a quelle convenzionali, nonché la maggiore attenzione prestata alla dimensione delle alleanze (nonostante il focus ancora prettamente bipolare) porta ad una più sofisticata riflessione sul processo psicologico attraverso cui la deterrenza può essere prodotta, non più visto come

[38] Robert Jervis, 'Deterrence Theory Revisited', and 'Rational Deterrence: Theory and Evidence', World Politics 42/2 (1989), 183-207.
[39] Glenn H. Snyder, 'Deterrence and Power', *The Journal of Conflict Resolution* 4/2 (June 1960), 163-178 e *Deterrence and Defense* (Princeton: Princeton University Press, 1961).
[40] Amos A. Jordan, Jr., 'Basic Deterrence and the New Balance of Power', *Journal of International Affairs* 14/1 (1960), 49-60. Si veda anche Morton A. Kaplan, *Some Problems in the Strategic Analysis of International Politics* (Princeton: Center for International Studies, 1959) e John Raser, 'Deterrence Research: Past Progress and Future Needs'.
[41] Jakub Grygiel and A Mitchell Wess, 'Limited War is Back', *The National Interest*, No. 135 (August 2014).

istantaneo.[42] La seconda ondata di ricerca dimostrò che, essendo l'esito di uno scontro convenzionale difficile da prevedere, le minacce deterrenti basate su capacità convenzionali risultavano inerentemente "contestabili" ovvero suscettibili di non essere credute da parte di coloro che ne erano fatti oggetto. A tale problema poteva ovviarsi ricorrendo a minacce nucleari per rafforzare l'inerentemente debole deterrenza convenzionale. La seconda ondata fece riferimento a tale fenomeno come "escalation", ovvero l'intensificazione o la diffusione di un inizialmente limitato uso della forza.[43] Le minacce deterrenti nucleari erano infatti per natura "incontestabili", ovvero non davano a chi ne era fatto oggetto, ragione di dubitare circa gli enormi costi che una determinata azione avrebbe comportato. Ciò ovviamente lasciando impregiudicata la questione della loro credibilità.[44] Il processo della deterrenza continuava dunque ad essere concepito come eminentemente psicologico, veniva tuttavia interpretato come più complesso, molto meno immediato e più legato alla capacità degli attori che attuavano una strategia di deterrenza di "segnalare" le proprie intenzioni e delineare i contorni della relazione di deterrenza che intendono instaurare.

La terza ondata iniziò ad emergere a partire dalla fine degli anni 60, ma prese realmente slancio negli anni 70, nello specifico nel 1974, a seguito della pubblicazione di un importante volume di Alexander George e Richard Smoke.[45] Le metodologie impiegate furono molto varie, modelli, metodi statistici e casi studio, ed il focus principale rimase il conflitto interstatale. Nonostante molti dei contributi riconducibili a questa ondata possano essere classificati, utilizzando la terminologia di Thomas Kuhn, come di "scienza normale", è possibile riscontrare alcune innovazioni degne di nota. Gli studiosi della terza ondata partirono dall'assunto che la deterrenza dovesse essere analizzata nel contesto geopolitico, storico, psicologico e culturale in cui le strategie venivano sviluppate.[46] Studi condotti da Robert Jervis, Ned Lebow, Janice Stein e Patrick Morgan, tra gli altri, svilupparono tale linea di ricerca.[47]

---

[42] William W. Kaufmann, "The Requirements of Deterrence," in William W. Kaufmann (ed.), *Military Policy and National Security* (Princeton: Princeton University Press, 1956), 12-38.
[43] I più importanti studi sull'argomento sono: Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960) *Thinking about the Unthinkable* (New York: Horizon Press, 1962); *On Escalation: Metaphors and Scenarios* (Westport: Praeger, 1965).
[44] James J. Wirtz, 'How Does Nuclear Deterrence Differ from Conventional Deterrence?', *Strategic Studies Quarterly* 12/4 (Winter 2018), 58-75.
[45] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy.*
[46] Paul C. Stern et al. (eds.), *Perspectives on Deterrence* (New York: Oxford University Press, 1989), 9
[47] Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, eds., *Psychology and Deterrence* (Baltimore: Johns Hopkins University Press, 1985).

Nonostante il focus a livello di attori rimanesse "diadico", la terza ondata non si concentra più, come invece quelle precedenti, sulle sole superpotenze, ma amplia la casistica ad attori statali in varie aree del mondo ed epoche storiche. Inoltre, l'attenzione si sposta in maniera definitiva, in termini di capacità analizzate, in ambito convenzionale. Particolarmente numerosi furono gli studi tesi a testare empiricamente il corpus di teoria elaborato in ambito nucleare su casi di deterrenza convenzionale.[48]

Per quanto concerne i meccanismi, la terza ondata esplorò ulteriormente sia la "punizione" che la "negazione", sottolineandone l'interazione nelle relazioni di deterrenza prolungata. In particolare per quanto riguarda la deterrenza *by denial* il meccanismo originariamente identificato negli studi dei primi anni 60 fu declinato con maggiore chiarezza. Si evidenziò infatti come dissuadere un'azione considerata dannosa mostrando all'avversario una capacità credibile di impedirgli di ottenere potenziali guadagni adeguati a motivare la stessa, non consistesse nel mero "blocco" di una o più opzioni disponibili all'avversario/competitore. Al contrario, diversi studi conclusero che, perché il meccanismo si attivasse, fosse necessario ridurre o modificare le opzioni al punto tale da costringerlo ad operare in ambiti non congeniali ed in modi non familiari.[49] Un esempio potrebbe essere l'approccio suggerito da alcuni esperti americani contemporanei per dissuadere la Cina dal tentare di occupare militarmente isole nel Mar Cinese meridionale. Secondo questo punto di vista, al fine di generare deterrenza per negazione, di USA dovrebbero sfruttare il vantaggio competitivo di cui dispongono a livello di sottomarini d'attacco, mantenendo un ritmo sostenuto nella costruzione di sottomarini classe Virginia in grado di negare alla Cina la possibilità di rifornire le proprie forze armate sulle isole eventualmente occupate. Alla luce delle limitate capacità di guerra antisommergibile di cui dispone, Pechino si troverebbe infatti costretta o ad operare in condizioni di estremo rischio o a dover affrontare oneri considerevoli per colmare il divario in questo campo.[50]

Lo stesso dibattito sulle famose capacità anti-access/area denial (A2/AD) deriva dallo

---

[48] Richard Betts, 'Conventional Deterrence', *World Politics* 37/2 (January 1985), 153-79; John Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983); Yair Evron, *War and Intervention in Lebanon: The Israeli-Syrian Deterrence Dialogue* (London: Routledge, 1987), 177; Johnathan Shimshoni, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988), 25.

[49] Samuel P. Huntington, 'Conventional Deterrence and Conventional Retaliation in Europe', *International Security* 8/3 (Winter 1983-1984), 32-56.

[50] Owen R. Cote' Jr., "Assessing the Undersea Balance between the United States and China," Thomas G. Mahnken (ed.), *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Palo Alto: Stanford University Press, 2012), pp. 184-205: Andrew S. Erickson, 'Deterrence by Denial: How to Prevent China From Using Force', *the National Interest*, December, 16, 2013 https://nationalinterest.org/commentary/war-china-two-can-play-the-area-denial-game-9564

sviluppo di sistemi volti a rendere estremamente costoso l'intervento avversario all'interno di certi perimetri.[51]

Tale prospettiva analitica portò inoltre a esplorare in maniera più approfondita il processo di deterrenza come combinazione di elementi psicologici e fisici.[52] In relazione alla componente psicologica, si evidenziò come la generazione di una reale influenza sul calcolo strategico dei potenziali avversari/competitori non potesse basarsi su astratte nozioni di razionalità teoricamente condivisa. Al contrario, la creazione di un effetto psicologico deterrente non poteva prescindere da un'adeguata conoscenza delle percezioni, psicologia e sistemi di valori degli avversari.[53] Detto altrimenti, a parità (o addirittura inferiorità) di capacità, la familiarità con la psicologia ed il sistema di valori di un avversario fornisce un notevole vantaggio competitivo ad ogni attore che porti avanti una strategia di deterrenza. Un esempio può essere il PD-59, il documento operativo di strategia nucleare approvato dall'amministrazione Carter nel 1980. In tale documento gli USA per la prima volta manifestavano la propria intenzione, nel corso di un conflitto nucleare, di dare la priorità alla decapitazione della leadership sovietica. Ciò alla luce di una serie di studi condotti in seno al National Security Council che avevano mostrato come la sopravvivenza dell'"avanguardia rivoluzionaria" e quella del partito comunista, rappresentassero il cuore del "sistema di valori" sovietico.[54]

Per quanto riguarda la componente fisica, la terza ondata non abbandonò (almeno inizialmente) l'assunto di partenza di un processo esclusivamente psicologico ereditato dalle ondate precedenti; il focus sulle capacità convenzionali tuttavia pose le basi perché tale assunto fosse gradualmente messo in discussione alla luce del fatto che il "fallimento" della deterrenza non avrebbe comportato alcun rischio di completa distruzione. Dunque,

---

[51] Andrew Krepinevich, Barry Watt and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessment, 2003); Robert Dalsjö, Christofer Berglund, Michael Jonsson, *Bursting the Bubble: Russian A2/AD in the Baltic Sea Region:Capabilities, Countermeasures, and Implications* (Stockholm: FOI, 2019).

[52] Paul Huth, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press 1988); Paul Huth and Bruce Russett, 'General Deterrence Between Enduring-Rivals: Testing Three Competing Models', *American Political Science Review* 87/1 (1993), 61-73; Janice Gross Stein, 'Deterrence and Learning in an Enduring Rivalry: Egypt and Israel 1948-73', *Security Studies* 6/1 (1996), 104-152.

[53] Robert Jervis, 'Perceiving and Coping with Threats', In Robert Jervis, Richard Ned Lebow, and Janice Gross Stein (eds.), *Psychology and Deterrence* (Baltimore: John Hopkins University Press, 1985); Richard Ned Lebow and Janice Gross Stein, 'Beyond Deterrence', *Journal of Social Issues* 43/4 (1987), 5-71 and 'The Elusive Variable', *World Politics* 42/3 (1990), 336-369. Si veda anche Jack S. Levy, 'Prospect Theory and International Relations: Theoretical Applications and Analytical Problems', *Political Psychology* 13/2 (1992), 283-310.

[54] Si veda: https://nsarchive2.gwu.edu/nukevault/ebb390/. Per una discussione degli aspetti concettuali si veda: Colin S. Gray, 'Nuclear Strategy: The Case for a Theory of Victory', *International Security* 4/1 (Summer, 1979), 54-87.

pur continuando a considerare ogni episodio di violenza nel quadro di una relazione deterrente come un "fallimento" della stessa, gli studiosi della terza ondata iniziarono a notare e porre in evidenza come di fatto tali fallimenti, ovvero l'attuazione della minaccia deterrente, contribuissero, a volte in maniera anche significativa, a definire con maggiore chiarezza i contorni delle relazioni di deterrenza, le cosiddette "regole del gioco".[55]

Nell'evoluzione del programma di ricerca della terza ondata inoltre, è possibile riscontrare un altro importante cambiamento che è stato spesso trascurato: la combinazione della deterrenza con altri strumenti di influenza. Pur mirando a condizionarne il calcolo strategico, una strategia di deterrenza lascia in ultima istanza all'avversario la decisione se essere o meno dissuaso. La terza ondata sottolineò come entrambi i meccanismi attraverso cui essa poteva operare si attivassero con maggiore probabilità in quei casi in cui le minacce deterrenti venivano accompagnate dall'impiego di incentivi positivi, strategie di rassicurazione e iniziative diplomatiche che in qualche modo contribuissero ad attenuare il conflitto stesso da cui l'esigenza di deterrenza nasceva.[56]

La Quarta Ondata, 2000-2009

Come la prima, la quarta ondata di teoria della deterrenza, è emersa in primo luogo in risposta a sviluppi reali, in particolare gli attacchi terroristici dell'11 Settembre 2001. Pur basandosi ampiamente su concetti elaborati in precedenza, la quarta ondata si caratterizza per una notevole discontinuità ed un significativo ampliamento del campo d'indagine. I principali aspetti teorici su cui i contributi inscrivibili al suo interno si sono concentrati sono: la dinamica del processo della deterrenza ed i suoi meccanismi di funzionamento in un ambiente complesso, caratterizzato da una molteplicità di attori e capacità diversificate.[57] La quarta ondata ha inoltre ulteriormente sviluppato istanze presenti nella terza ondata, dando origine a un concetto più ampio di deterrenza che include, ma non si limita, alle minacce di ritorsioni militari.[58]

---

[55] Jeffrey W. Knopf, 'Three Items in One: Deterrence as Concept, Research Program, and Political Issue', in T.V. Paul, Patrick Morgan, and James Wirtz (eds.), *Complex Deterrence*, 48; Frank P. Harvey, 'Rigor Mortis, or Rigor, More Tests: Necessity, Sufficiency, and Deterrence Logic', *International Studies Quarterly* 42 (December 1998), 675-707.

[56] Colin S. Gray, 'The Reformation of Deterrence: Moving On', *Comparative Strategy* 22/5 (December 2003), 429-461.

[57] Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research', 1-2; Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory-Toward a New Research Agenda', 705.

[58] T.V. Paul, 'Complex Deterrence: An Introduction'.

Per quanto riguarda il primo criterio, gli attori, la quarta ondata di teoria sulla deterrenza amplia in maniera significativa il campo di ricerca, sia in relazione al numero che alla tipologia. Diversi studi sottolineano come una serie di cambiamenti intervenuti nel sistema internazionale dalla fine della guerra fredda abbia inciso in maniera significativa sui percorsi della deterrenza.[59] Infatti, il sistema è caratterizzato da: un aumento dell'importanza degli attori non statali; una marcata tendenza ad una redistribuzione del potere militare per via della globalizzazione e di dinamiche ad essa collegate, quale la rivoluzione ICT (nonostante gli Stati Uniti mantengano una solida primato, il sistema non può essere del tutto definito unipolare); gerarchie di potere e status quo sempre più contestati ed instabili, tanto tra attori statali (ritorno della competizione tra grandi potenze), quanto tra attori statali e non-statali (interessati a modificare lo status quo regionale o internazionale).[60]

In un ambiente ben strutturato, con un numero di attori circoscritto coinvolto in relazioni di deterrenza, le parti imparano a conoscersi reciprocamente in tempi relativamente brevi, l'ambito delle relazioni di deterrenza è abbastanza semplice da definire, e ciò che può considerarsi "dentro" e "fuori" più facile da stabilire. Al contrario, l'indeterminatezza strutturale che caratterizza l'attuale sistema introduce un forte elemento di complessità nelle relazioni di deterrenza che si manifesta nella: segnalazione delle minacce, attribuzione di responsabilità per azioni ostili, e asimmetria degli interessi.[61] In un sistema strutturalmente indeterminato, caratterizzato da un numero elevato di attori di diversa natura con rapporti di potere fluidi e contestazioni allo status quo di incerta natura, diventa infatti molto più difficile tanto definire le condizioni di portata di una strategia di deterrenza, ovvero le "regole del gioco", quanto codificarne e renderne stabili le pratiche.[62]

---

[59] Ian R. Kenyon and John Simpson (eds.), *Deterrence and the New Global Security Environment* (London: Routledge, 2006).

[60] Stephen G. Brooks and William C. Wohlforth, 'The Rise and Fall of the Great Powers in the Twenty-first Century: China's Rise and the Fate of America's Global Position', *International Security* 40/3 (Winter 2015/16), 7-53; Hal Brands, *American Grand Strategy in the Age of Trump* (Washington DC: Brookings Institution Press, 2018).

[61] Karl P. Mueller, 'Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century', *Strategic Studies Quarterly* 12/4 (Winter 2018), 76-93.

[62] Patrick Morgan and T.V. Paul, 'Deterrence among Great Powers in an Era of Globalization' and Janice Gross Stein, '*No Common Knowledge*' entrambi in in T.V. Paul, Patrick Morgan, and James Wirtz (eds.), *Complex Deterrence*, 259–279 e 59; Sebastian Rosato, 'The Inscrutable Intentions of Great Powers' *International Security* 39/3 (Winter 2014/15) 48-88; Charles L. Glaser, Andrew H. Kydd, Mark L. Haas, John M. Owen IV and Sebastian Rosato, 'Correspondence: Can Great Powers Discern Intentions?', *International Security* 40/3 (Winter 2015/16), 197-215.

In relazione alla tipologia di attori, per le ragioni in precedenza discusse, la quarta ondata si focalizza principalmente sulla deterrenza di attori non-statali.[63] Sotto questo punto di vista un contributo importante riguarda l'abbandono della prospettiva razionalista e unitaria che aveva caratterizzato le precedenti ondate di teoria, concentrate sulla deterrenza inter-statale.[64] Una serie di ricerche condotte dalla RAND Corporation, in particolare da Paul Davis e Brian Jenkins, evidenzia infatti la necessità di concettualizzare gli attori coinvolti nelle relazioni di deterrenza, in particolare quelli non statali, come sistemi complessi articolati in un insieme di sub-elementi in costanti e fluide interazioni, più che come entità monolitiche. Secondo gli autori, tale concettualizzazione è essenziale al fine di comprendere in maniera adeguata non solo come gli attori non statali ricevono informazioni dall'ambiente esterno, ma anche come le trasmettono ed elaborano all'interno. Le modalità di recezione, trasmissione ed elaborazione delle informazioni condizionano infatti non solo le motivazioni e percezioni di ognuna delle sub-componenti di un sistema/attore non statale, ma il suo processo decisionale e calcolo strategico ad un macro-livello.[65] Un esempio in merito può essere considerato il dibattito che ebbe luogo tra i noti studiosi Bruce Hoffman e Marc Sageman circa l'efficacia della "decapitazione" di al-Qaeda, in cui la questione della struttura dell'organizzazione ed i suoi modelli di decision-making occuparono un ruolo centrale.[66]

In relazione al secondo aspetto preso in considerazione in questo elaborato, le capacità, la quarta ondata ancora una volta si caratterizza per una significativa discontinuità con la precedente teoria della deterrenza. Emerge infatti un consenso quasi unanime tra i più rilevanti studi circa la necessità di esplorare il nesso tra la deterrenza

---

[63] Robert Trager and Dessislava Zagorcheva, 'Deterring Terrorism', *International Security* 30/3 (Winter 2005/06), 87-123.

[64] Alexander L. George, 'The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries', *Comparative Strategy* 22/5 (December 2003), 465; Neil J. Smelser and Faith Mitchell (eds.), *Discouraging Terrorism: Some Implications of 9/11*, National Research Council study (Washington DC: National Academies Press, 2002); Wyn Q. Bowen, 'Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism', *Contemporary Security Policy*, 25/1 (April 2004), 58, 65, 67.

[65] Paul K. Davis Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism A Component in the War on al Qaeda* (Santa Monica: RAND, 2002); Paul K. Davis Brian Michael Jenkins, 'A System Approach to Deterring and Influencing Terrorists', *Conflict Management and Peace Science* 21/1 (2004), 3-15; Shaul Mishal & Maoz Rosenthal, 'Al Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations' *Studies in Conflict & Terrorism* 28/4 (2005), 275-293.

[66] Bruce Hoffman & Marc Sageman, 'Does Osama Still Call the Shots? Debating the Containment of Al Qaeda's Leadership', *Foreign Affairs*, 87/4 (July/August 2008), 163–166; si veda anche: Jenna Jordan, 'Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes', *International Security* 38/4 (Spring 2014), 7–38 e Patrick B. Johnston, "Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns," *International Security*, Vol. 36, No. 4 (Spring 2012), 47-79.

come *outcome* e combinazioni di capacità.[67] Tale orientamento può dirsi sintetizzato nel concetto di "deterrenza su misura" (*tailored deterrence*), introdotto nel lessico strategico della teoria della deterrenza in alternativa a quella che è stata definita la "one-size-fits-all deterrence" (caratteristica della guerra fredda), al fine di illuminare possibili collegamenti tra l'impiego nelle strategie di deterrenza di una pluralità di capacità, militari e non, specificamente adattate per avversari/competitori. [68] Nonostante il consenso rispetto all'idea generale di adattare le strategie di deterrenza a specifici avversari, gli studi della quarta ondata manifestano un certo disaccordo in relazione alla tipologia di capacità da incorporare. Infatti, se per alcuni il *tailoring* avrebbe dovuto limitarsi alle capacità militari, la maggioranza sembra più propensa a prendere in considerazioni varie tipologie di capacità, cinetiche e non, ovvero anche strumenti informativi, diplomatici ed economici a scopi coercitivi e di influenza.[69] Inoltre, alcuni studiosi hanno sollevato dubbi circa la realistica possibilità di influenzare in modo decisivo il calcolo strategico ed il processo decisionale di un avversario attraverso combinazioni specifiche di capacità. Secondo tale orientamento gli avversari/competitori non possono essere immaginati come sistemi inerti e vulnerabili a forme di condizionamento finemente elaborate; operando la deterrenza in maniera piuttosto rozza, come un martello più che un bisturi, sarebbe estremamente complesso comprendere attraverso il frastuono e la "nebbia" della politica internazionale esattamente quale componente capacitiva influenzi l'avversario.[70] Max Abrahms e Philip Potter, per esempio, hanno spiegato come la decapitazione della leadership di un gruppo terroristico possa portare a più o meno violenza, da parte di quest'ultimo, a seconda della sua struttura interna.[71]

---

[67] Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004), 58-59; Michael Quinlan, 'Deterrence and Deterrability', *Contemporary Security Policy*, 25/1 (April 2004) 12; Jerrold M. Post, 'Deterrence in an Age of Asymmetric Rivals', in Stanley A. Renshon and Peter Suedfeld (eds.), *Understanding the Bush Doctrine* (New York: Routledge, 2007), 158.

[68] Austin Long, 'Deterrence: The State of the Field', *NYU Journal of International Law and Politics* 47/2 (Winter 2015): 357-377 http://nyujilp.org/wp -content/uploads/2015/11/NYI204.pdf. Si veda anche: Karl-Heinz Kamp and David S. Yost (eds.), *NATO and 21st Century Deterrence*, NDC Forum Paper 8 (Rome: NATO Defense College, May 2009).

[69] M. Elaine Bunn, 'Can Deterrence be Tailored?', *Strategic Forum* no. 255 (January 2007), 5; John Baylis, 'The Concept of 'Tailored Deterrence' in the 'Second Nuclear Age'', *St Antony's International Review*, 4/2 (February 2009), 8-23. Per una prospettiva ancora più ampia si veda anche Van Jackson, 'Beyond Tailoring: North Korea and the Promise of Managed Deterrence', *Contemporary Security Policy* 33/2 (2012), 289-310.

[70] Colin S. Gray, *Strategy and Defence Planning: Meeting the Challenge of Uncertainty* (Oxford: Oxford University Press, 2016), 130; Sean P. Larkin, *Cracks in the New Jar: The Limits of Tailored Deterrence* (Carlisle: US Army War College, 2011), 25; Patrick Morgan, 'Evaluating Tailored Deterrence', in Karl Heinz Kamp & David S. Yost (eds.), *NATO and 21st Century Deterrence*.

[71] Max Abrahms and Philip B.K. Potter, "Explaining Terrorism: Leadership Deficits and Militant Group Tactics," *International Organization*, Vol. 69, No. 2 (Spring 2015), pp. 311-342.

Anche sotto il profilo dei meccanismi della deterrenza la discontinuità tra la quarta ondata e i precedenti contributi è considerevole. Viene infatti identificato un nuovo meccanismo attraverso cui rendere la deterrenza operativa, che va ad aggiungersi ai due già noti di *punishment* e *denial*: deterrenza attraverso delegittimazione (*delegitimization*), anche nota come "deterrenza attraverso contraccolpo pubblico" (by *public backlash*) o ancora "deterrenza attraverso contro-narrativa" (*counter-narrative*). Il fattore chiave di questo meccanismo di deterrenza sarebbe l'utilizzo di informazioni, la costruzione di narrative, in altre parole la comunicazione strategica, al fine di delegittimare, di frammentare, il consenso di cui un avversario gode rispetto ad un certo corso d'azione ritenuto minaccioso.[72] Più precisamente in tale meccanismo il calcolo strategico di un avversario/competitore viene modificato attraverso la manipolazione dei motivi e delle giustificazioni che ne informano le preferenze.[73] L'identificazione di tale meccanismo è derivata dall'osservazione che numerose organizzazioni terroristiche e insurrezionali risultavano particolarmente sensibili al grado di consenso riscosso dalle proprie scelte strategiche e tattiche tra i gruppi sociali di riferimento.[74] La realizzazione che queste ultime, in effetti, rappresentassero un "centro di gravità", ha suggerito la possibilità che tale legame potesse essere utilizzato come leva per attivare un precedentemente sconosciuto meccanismo di deterrenza.[75] E' stato fatto notare tuttavia come l'attivazione di questo meccanismo sia piuttosto complessa in particolare a causa di potenziali contraccolpi. Il tentativo da parte di un attore di delegittimare un avversario di fronte ai propri sostenitori potrebbe infatti provocare, per reazione, un rafforzamento di istanze di "rally around the flag".[76]

In relazione al processo della deterrenza, la quarta ondata sviluppa una concezione più complessa delle precedenti. Come già sottolineato, nelle prime tre ondate di teoria, la

---

[72] Alex Wilner 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies* 34/1, (2011), 3-37.

[73] Jerry Mark Long & Alex Wilner, 'Delegitimizing al-Qaida: Defeating an 'Army Whose Men Love Death', *International Security* 39/1 (Summer 2014), 126-164; si veda anche: Miroslav Nincic, Getting What You Want: Positive Inducement in International Relations, *International Security* 35/1 (Summer 2010), 138-183.

[74] Joseph Lepgold, 'Hypotheses on Vulnerability: Are Terrorists and Drug Dealers Coercable?', in Lawrence Freedman (ed.), *Strategic Coercion: Concepts and Cases* (New York: Oxford University Press, 1998), 136, 145.

[75] Brad Roberts, 'Deterring Terrorism: Terrorist Campaigns and Prolonged Wars of Mutual Coercion', in Institute for Defense Analyses, *Deterring Terrorism: Exploring Theory and Methods* (Alexandria: Institute for Defense Analyses, August 2002), IV-23–IV-24; Brad Roberts, *Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction* (Alexandria: Institute for Defense Analyses, June 2007), 18; Lewis A. Dunn, 'Can al Qaeda Be Deterred from Using Nuclear Weapons?', Occasional Paper 3, Center for the Study of Weapons of Mass Destruction (Washington DC: National Defense University Press, July 2005), 2, 11.

[76] Adam Garfinkle, 'Does Nuclear Deterrence Apply in the Age of Terrorism?', *Footnotes: The Newsletter of FPRI's Wachman Center* 14/10 (May 2009).

deterrenza veniva concepita come un processo psicologico, immediato o relativamente rapido, legato alla percezione della potenza materiale di un attore.[77] Elaborando critiche già in precedenza avanzate da diversi studiosi,[78] nella quarta ondata si sottolinea come deterrenza sia da intendersi come un processo complesso, possibilmente anche lento, di interazione, tanto fisica quanto psicologica, tra le parti.[79]

L'esecuzione di una strategia di deterrenza si basa, secondo molti studi della quarta ondata, anzitutto sulla capacità di diffondere la propria interpretazione della relazione di deterrenza. Tali analisi hanno infatti avanzato l'ipotesi che, in termini cognitivi, il processo di deterrenza richieda più della mera comunicazione della minaccia. Secondo tale punto di vista, una strategia deve infatti includere la definizione di regole e pratiche che risultino comprensibili agli attori verso cui la strategia è diretta. Ciò allo scopo di "aiutare" avversari/competitori, che non necessariamente condividono la stessa nozione di deterrenza, ad interpretare in maniera corretta azioni e messaggi. In altre parole essenziale è che chi adotta una strategia di deterrenza si sforzi di definirne i contorni, di elucidare le regole del gioco al fine di evitare che gli avversari recepiscano le minacce dissuasive come semplici "provocazioni".[80]

L'elemento psicologico-comunicativo deve inoltre essere coordinato con quello fisico. Sviluppandosi principalmente in risposta a problemi relativi alla deterrenza di attori non statali e contesti di conflitti asimmetrici, diversamente dalle ondate precedenti, numerosi studi della quarta ondata concepiscono il processo di deterrenza come implicante anche periodici usi della forza.[81] In tale visione, l'attuazione di una minaccia non rappresenta infatti un "fallimento" e nemmeno, come sottolineato da molti dei contributi delle tre ondate precedenti, un atto retroattivo di punizione retributiva. Al contrario, l'attuazione della minaccia rappresenta un'azione utilitaria lungimirante, finalizzata sia a punire nell'immediato la violazione delle "regole del gioco", sia ad influenzare il calcolo

[77] Derek D. Smith, *Deterring America: Rogue States and the Proliferation of Weapons of Mass Destruction* (New York: Cambridge University Press, 2006) 25.

[78] Joseph Nye, 'Nuclear Learning and the US-Soviet Security Regime', *International Organization* 41/3 (1987), 371-402; Jack Levy, 'Learning and Foreign Policy: Sweeping a Conceptual Minefield', *International Organization* 48/2 (1994), 279-312.

[79] Timothy W. Crawford, 'Pivotal Deterrence and the Kosovo War: Why the Holbrooke Agreement Failed', *Political Science Quarterly* 116/4 (2002), 499-523 and *Pivotal Deterrence: Third-Party Statecraft and the Pursuit of Peace* (Ithaca: Cornell University Press, 2004).

[80] Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda', 722.

[81] Colin S. Gray, *Maintaining Effective Deterrence* (Carlisle: US Army War College, August 2003), 7.

decisionale dell'avversario imponendo un costo abbastanza elevato da scoraggiare attacchi futuri.[82]

Il processo di deterrenza, così come emerge dagli studi della quarta ondata, può dunque essere inteso come un lento processo psico-fisico di generazione nell'avversario/competitore di "conoscenza", relativa a valori, capacità e circostanza in cui i primi saranno tutelati attraverso l'impiego delle seconde. Un attore che mette in atto una strategia di deterrenza non deve solo comunicare le proprie intenzioni strategiche in maniera generale, ma manifestare con chiarezza come tali idee potrebbero essere attuate ed in quali circostanze.

La Quinta Ondata 2007-2016

Non esiste consenso tra gli studiosi circa l'esistenza di una "quinta ondata" di teoria della deterrenza.[83] L'opinione qui sostenuta tuttavia è che, alla luce di quella che è la natura dei più recenti contributi in materia, essi non possano più essere considerati come parte della "quarta ondata". Al contrario, si ritiene che vadano a configurarsi come un nuovo blocco, contraddistinto da caratteristiche proprie.

La maggior parte degli studi della "quinta ondata" sono focalizzati sul dominio cyber. Essi analizzano le condizioni fondamentali per il successo della deterrenza, i problemi relativi allo sviluppo e impiego di capacità offensive e difensive, le questioni connesse alla credibilità della minaccia ed alla capacità di trasmettere il messaggio deterrente.[84]

Il concetto di deterrenza cyber ha origine già negli anni '90 sulla base di simulazioni e 'wargames' condotti al Dipartimento della Difesa degli Stati Uniti. E' nel 2007 tuttavia, a seguito della campagna di attacchi 'distributed denial of service' (DDS) condotta contro l'Estonia, che si può dire abbia avuto inizio una nuova ondata di teorizzazione che ha poi raggiunto il culmine durante il periodo compreso tra il 2013 al 2016. Negli ultimi 5 anni

---

[82] Alex Wilner, 'Contemporary Deterrence Theory and Counterterrorism: A Bridge too Far?' *NYU Journal of International Law and Politics* 47/2 (2015).

[83] Dmitry (Dima) Adamsky, 'From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies*, 41/1-2 (2018), 33-60; Tim Prior, 'Resilience: The 'Fifth Wave' in the Evolution of Deterrence', in Oliver Thränert, Martin Zapfe (eds.) *Strategic Trends 2018: Key Developments in Global Affairs* (Zurich: Center for Security Studies ETH Zurich, 2018), 63-79.

[84] Richard J. Harknett, 'Information Warfare and Deterrence', *Parameters* 26/3 (1996), 93-107; Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington, DC: National Defense University Press, 1996), v-vi, 5-6; Bruce D. Berkowitz, 'Warfare in the Information Age', in John Arquilla and David F. Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997), 183-184; Emily O. Goldman, 'Introduction: Security in the Information Technology Age', John Arquilla, 'Thinking about New Security Paradigms', both in Emily O. Goldman (ed.), *National Security in the Information Age* (New York: Routledge, 2004), 3, 210-213. Per un approccio diverso si veda: Lior Tabansky, 'Basic Concepts in Cyber Warfare', *INSS Military and Strategic Affairs* 3/1 (2011), 75-92.

il concetto è diventato sempre più controverso e dibattuto e, da parte di alcuni studiosi, è stato considerato addirittura irrilevante e sostanzialmente non applicabile come strumento di policy.

Le ragioni che hanno portato ad un ridimensionamento dell'importanza del concetto di deterrenza cyber sono di vario tipo, ma risiedono soprattutto nella peculiare natura del dominio.[85] Il dominio cyber può essere descritto in termini di tre livelli: rete fisica, rete logica e cyber-persona. Il livello della rete fisica è, molto semplicemente, l'infrastruttura su cui viaggiano i dati. Il livello di rete logica è costituito da quegli elementi della rete la cui interrelazione prescinde dalla dimensione fisica, come ad esempio un sito Web ospitato su server in più posizioni fisiche in cui è possibile accedere a tutti i contenuti attraverso un unico localizzatore di risorse. L'ultimo livello, il più astratto, è quello della cyber-persona. Sulla base delle regole che si applicano nella rete logica, in questo livello si sviluppano rappresentazioni digitali, le identità, di individui ed entità nel cyberspazio.[86] Tale struttura consente ad ogni attore che operi nel dominio cyber la capacità di modificare tanto la propria identità, quanto la propria collocazione geografica, in altre parole di operare in condizioni di clandestinità/ambiguità.[87] Quest'ultima risulta poi ancor più pronunciata alla luce della possibilità, generata dalle basse barriere di entrata nel dominio cyber, per gli attori statali di utilizzare attori non-statali, e finanche individui come *proxies* e *cutouts* per mantenere un elevato livello di *plausible deniability*.[88]

Tali caratteristiche del dominio cyber contribuiscono a rendere la deterrenza molto più complessa. Le strategie di deterrenza si fondano in primo luogo sull'identificazione dell'avversario/competitore al fine di renderlo consapevole delle conseguenze dell'azione che si intende dissuadere, procedura particolarmente difficile nel dominio cyber, anche *ex post*.[89] Si pensi ad esempio all'applicabilità del famoso modello di "brinkmanship". Questo modello si basa su una chiara identificazione dell'aggressore nonché su una dimostrabile capacità di ritorsione ed una certa credibilità. Capacità e

---

[85] Andrew Chadwick, & Philip Howard (Eds.), *Routledge Handbook of Internet Politics* (London: Routledge 2009).

[86] US Department of Defense, *Joint Publication 3-12: Cyberspace Operations* (Washington DC: Department of Defense, 2018) https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[87] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009), 43-45; Robert Mandel, *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks* (Washington DC: Georgetown University Press, 2017), 9.

[88] Erica D. Borghard and Shawn W. Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies?', *Orbis* 60/3 (2016), 395-416; Aaron F. Brantly, 'Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace', *Intelligence and National Security* 31/5 (2015), 674-685.

[89] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38/1-2 (2015), 4-37; Charles Glaser, 'Deterrence of Cyber Attacks and U.S. National Security', GW-CSPRI no. 5 (2011).

credibilità non necessariamente rappresentano un problema nel dominio cyber, ma l'evidente difficoltà nell'individuare l'attaccante complica in maniera considerevole la valutazione strategica di costi e benefici, rende difficile comprendere la strategia della controparte, nonché la sua percezione dei 'guadagni' e le sue preferenze, sostanzialmente invalidando l'intero modello e rendendolo inapplicabile al dominio cyber.[90]

La difficoltà di identificazione del "bersaglio" della minaccia nel dominio cyber rende la deterrenza problematica anche sotto un secondo profilo. Essa incide infatti sulla possibilità di adattare le capacità alla base della stessa, costringendo in una certa misura un attore che porti avanti una strategia di deterrenza nel dominio cyber a decidere sul momento il "pacchetto" capacitivo da impiegare. [91] Altrettanto problematica è la "segnalazione" (*signaling*), data la segretezza delle operazioni informatiche e la difficoltà di discernere tra comportamenti offensivi e difensivi. Da ultimo, alla luce della pluralità di attori operanti in questo dominio, nonché del più probabile impiego di *proxies* e *cutouts*, l'assunto di comportamento razionale caratteristico di larga parte della teoria della deterrenza non può darsi per scontato.[92]

Dopo questa premessa generale è possibile passare all'analisi di quelle che possono essere considerate le novità fondamentali che caratterizzano la quinta ondata. Esse sono: l'identificazione di almeno tre nuovi meccanismi di possibile funzionamento della deterrenza, un approccio sinergico all'impiego delle capacità nei vari domini, e una concettualizzazione più sofisticata più della combinazione degli elementi psicologico e fisico nel processo della deterrenza.

Per quanto riguarda gli attori il focus sulla dimensione cyber che caratterizza la quinta ondata ha generato un focus sulla questione della "ambiguità" nelle relazioni di deterrenza. Nella teoria della deterrenza tale questione non rappresenta un'assoluta novità, già nel 1960 infatti Thomas Schelling aveva discusso la nozione della "minaccia che lascia qualcosa al caso"; la quinta ondata di teoria della deterrenza ha tuttavia in un primo momento sottolineato come il cyberspazio generasse sotto questo profilo rischi ed opportunità senza precedenti. Diversi studiosi, soprattutto nei primi anni di teorizzazioni,

---

[90] Mariarosaria Taddeo, 'On the Risks of Relying on Analogies to Understand Cyber Conflicts', *Minds and Machines*, 26/4 (2016), 317–321; David Betz, & Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue,* 44/*2* (2013), 147–164.

[91] Per una discussione del concetto di "deterrenza adattata" nel dominio cyber si veda: Richard L. Kugler, 'Deterrence of Cyber Attacks', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington DC: National Defense University Press, 2009), 331-33 e Martin C. Libicki, *Conquest in Cyberspace* (Cambridge, Cambridge University Press, 2007), 272.

[92] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard UP, 2020), 3-4.

hanno sottolineato come le numerose ambiguità tattiche del dominio cyber diano spazio a ipotesi di strategie di deterrenza intrinsecamente basate sulla "opacità" ovvero sulla possibilità di negare la responsabilità per minacce ed azioni (anche quando se ne è autore) rivendicandola poi per altre (anche qualora non responsabili).[93] Il vantaggio che ne deriverebbe sarebbe complicare il calcolo strategico dell'avversario o "bersaglio", rendendolo cauto al punto di paralizzarlo. Per quanto in linea di principio plausibile, diversi studi hanno giudicato un esito di questo tipo improbabile. E' stato infatti sottolineato come sviluppare una strategia di deterrenza fondata su una completa ambiguità circa azioni e responsabilità (sfruttando la struttura a tre livelli del dominio cyber) non sia realisticamente possibile. Si richiederebbe infatti in ogni caso rivelare informazioni (e dunque non essere troppo ambigui) circa le proprie capacità, il che a sua volta invaliderebbe l'opacità, consentendo attribuzione di responsabilità per "associazione di capacità".[94]

Proprio in relazione alla questione delle capacità, la quinta ondata ha introdotto innovazioni significative. In un primo momento sembrò che le capacità cyber fossero ideali per lo sviluppo ed attuazione di strategie di deterrenza e più in generale di coercizione per molteplici motivi: le capacità cyber sono "scalabili" e consentono notevole "precisione", i loro effetti possono essere facilmente adattati alle esigenze della situazione e la natura del "bersaglio". Possono inoltre rimpiazzare capacità più "costose" come la forza militare o sanzioni economiche.[95]

Tali aspettative sono poi state ridimensionate: la natura "clandestina" delle capacità ne rende l'uso nel quadro di strategie di deterrenza complicato. Come hanno dimostrato diversi recenti studi, esiste un non trascurabile trade-off tra i vantaggi di mantenere segreto un certo tipo di capacità e rivelare alcune informazioni su di esso a scopo deterrente.[96] Il problema del *quantum* di informazioni da rivelare è suscettibile di

---

[93] Martin C. Libicki, 'The Strategic Uses of Ambiguity in Cyberspace', *INSS Military and Strategic Affairs*, 3/3 (December 2011), 3-10.

[94] Aaron F. Brantly, 'Ambiguous Deterrence', *The Cyber Defense Review*, January 23 2016 https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136127/ambiguous-deterrence; David Blagden, 'Deterring Cyber Coercion: The Exaggerated Problem of Attribution', *Survival Global Politics and Strategy*, 62/1 (2020), 131-148.

[95] David Gompert and Martin Libicki, 'Waging Cyber War the American Way', *Survival* 57/4 (2015); Max Smeets and Herbert S. Lin, 'Offensive Cyber Capabilities: To What Ends?', in Tomáš Minárik, Raik Jakschis, and Lauri Lindstrom (eds.), *2018 10th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2018).

[96] Brendan Rittenhouse Green & Austin Long, *The Role of Clandestine Capabilities in Deterrence: Theory and Practice* (U.S. Naval Postgraduate School Project on Advanced Systems and Concepts for Countering WMD Final Report September 2017).

invalidare completamente una strategia di deterrenza; un'operazione cyber di impiego limitato di tale capacità con finalità di deterrenza potrebbe passare o del tutto inosservata, o essere erroneamente interpretata come un attacco. Inoltre, come ha osservato Robert Jervis potrebbe anche accadere che: "l'attore oggetto dell'attacco supponga che l'effetto prodotto da un attacco fosse quello voluto".[97]

Eppure, i problemi sopra esposti hanno portato un certo numero di ricercatori a sottolineare come la deterrenza nel cyberspazio non necessariamente debba basarsi esclusivamente su capacità cyber, escludendo capacità "tradizionali".[98] Aaron Brantly, ad esempio, ha sostenuto nel 2018 che la principale sfida non è definire la deterrenza nel cyberspazio, ma comprendere il ruolo che le tecnologie digitali giocano nella più ampia portata della deterrenza ampiamente intesa.[99] L'assunto di partenza è che la deterrenza in un dominio raramente, se non mai, opera indipendentemente da altri domini e a prescindere dall'intero spettro di capacità di cui gli attori coinvolti nella relazione di deterrenza dispongono.[100] Pertanto, è stato suggerito come la deterrenza di attacchi cyber da parte di attori statali potrebbe basarsi su capacità economiche e militari, mentre per quanto riguarda la deterrenza di minacce cyber poste da individui o organizzazioni terroristiche sarebbe più opportuno ricorrere a strumenti giudiziari (interni o internazionali) e di polizia o servizi di sicurezza interni.[101] In sostanza, le scelte relative al tipo di capacità da impiegare per esercitare deterrenza nel cyberspazio dipendono dalla valutazione di un attore dei potenziali vantaggi derivanti dal deviare o meno lo scontro da quel dominio.[102]

Il dibattito su questioni relative a conflitto e competizione nel cyberspazio ha promosso anche quella che probabilmente è la più ampia riconcettualizzazione della nozione di deterrenza da quando il termine è stato introdotto nel vocabolario strategico occidentale. Diversi esperti hanno infatti sottolineato come la crescente complessità

---

[97] Robert Jervis, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare*, 15/2 (2016).

[98] Martin C. Libicki, 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly* 12/4 (Winter 2018), 46.

[99] Aaron F. Brantly, 'The Cyber Deterrence Problem'.

[100] Aaron F. Brantly, 'The Cyber Deterrence Problem' in *The 10th International Conference on Cyber Conflict* (Tallinn: NATO Cyber Defense Center of Excellence, 2018), 31–54; Shawn Henry and Aaron F. Brantly, 'Countering the Cyber Threat', *The Cyber Defense Review* 3/1 (Spring 2018), 47-56.

[101] Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence,* 13, 19-20; Richard Kugler, 'Deterrence of Cyber Attacks', 328; Antony Cordesman & Justin Cordesman, Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland (Washington DC: CSIS, 2002), 7.

[102] Patrick Morgan, 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in John D. Steinbruner et al. (eds.) *Proceedings of a Workshop on Deterring Cyberspace: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010), 59.

socio-tecnologica del contesto entro cui le strategie di deterrenza operano richiede una visione più articolata della nozione generale.[103] Tale orientamento appare sintetizzato nel concetto di "deterrenza tra dominii" (*cross-domain deterrence*). Di tale concetto esistono due definizioni. La prima più semplice sembra da intendersi come riferita al contrasto di minacce in un'arena (come lo spazio o il cyberspazio) attraverso una tipologia diversa di capacità (come il potere marittimo o anche strumenti non militari, come l'accesso al mercato) in cui si ritiene che le minacce deterrenti possano essere più efficaci. Si tratterebbe in altre parole di una concettualizzazione asimmetrica delle capacità alla base della deterrenza consistente nello sfruttamento di aree capacitive in cui si gode di un vantaggio comparativo per compensare eventuali debolezze in altri settori. Gli esempi potrebbero includere l'uso del potere aereo per rispondere a terrorismo o di interruzioni informatiche del comando e controllo militari. La recente risposta militare israeliana, tramite l'aeronautica, ad un attacco cibernetico, rientrerebbe anch'essa in questa categoria.[104]

Una seconda definizione del concetto esistente in letteratura appare invece più ampia. Essa parte da una concettualizzazione della nozione di "dominio" piuttosto differente da quella adottata dalla comunità di difesa USA già alla fine della prima decade degli anni 2000.[105] Un "dominio" non deve infatti essere inteso necessariamente come un ambito geografico. Al contrario, tale definizione emergente abbraccia una nozione molto più ampia e fondamentalmente indipendente dalla dimensione geografica, ovvero quella di dominio come qualsiasi percorso o mezzo di coercizione con caratteristiche proprie, peculiari, sufficientemente diverso da altre capacità sia sotto il profilo materiale, che in termini di impatto politico. Le armi nucleari e convenzionali possono quindi essere considerate domini diversi a causa delle loro caratteristiche materiali e politiche profondamente diverse, anche se entrambi i tipi di forze sono dispiegati negli ambienti terrestri, marittimi, aerei e spaziali.[106]

---

[103] James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge: Harvard University Press, 1986); Douglass C. North, *Institutions, Institutional Change, and Economic Performance* (New York: Cambridge University Press, 1990); Joel Mokyr, *The Gifts of Athena: Historical Origins of the Knowledge Economy* (Princeton: Princeton University Press, 2002).

[104] Erica D. Borghard and Jacquelyn Schneider, 'Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal.', *Washington Post Monkey Cage*, May, 19, 2019.

[105] Vincent Manzo, 'Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?', *Strategic Forum*, no. 272 (December 2011), 3.

[106] Eric Garztke and Jon Lindsay, "Cross-Domain Deterrence: Strategy in an Era of Complexity," working paper, University of California Institute on Global Conflict and Cooperation (IGCC), 15 July 2014; Austin Long, 'Deterrence: The State of the Field', 358.

A livello teorico, l'introduzione del concetto di deterrenza *cross-domain* ha aperto la strada ad una delle riflessioni più significative relative al funzionamento del fenomeno della deterrenza dai tempi della seconda ondata. E' stato infatti evidenziato come il percorso della deterrenza non debba essere inteso esclusivamente come orizzontale, così come rappresentato sin dagli anni 60. Al contrario la più ampia concettualizzazione del fenomeno implicita nella nozione di deterrenza *cross-domain* evidenzia l'esistenza di una dimensione orizzontale ed una conseguente possibilità di *escalation* laterale. Ciò in pratica equivale alla possibilità di obbligare un avversario/competitore, dissuadere un corso d'azione, non solo con minacce di intensificazione di uso della forza *all'interno* di un dominio, ma attraverso un percorso di escalation verticale *attraverso* i domini. Tale modello differisce dall'*escalation* tradizionale, in cui chi attua una strategia di deterrenza intensifica il confronto a seguito della violazione da parte del "bersaglio" di una particolare "soglia", ovvero a seguito del rifiuto di conformarsi ad una richiesta. Nell'*escalation* laterale chi attua una strategia di deterrenza si muove invece tra i vari domini anche indipendentemente dal raggiungimento di determinate soglie, in base a dove in ogni particolare momento gode di un vantaggio competitivo, al fine di mantenere l'iniziativa ed il pieno controllo del processo di *escalation*. L'escalation laterale non rappresenta una novità assoluta, la famosa dottrina della "massive retaliation" sviluppata dall'Amministrazione Eisenhower potrebbe essere considerata un esempio di escalation laterale nella misura in cui si minacciavano i sovietici di rappresaglie "with means of our own choosing". La differenza principale con la formulazione più recente ricompresa nella "cross-domain deterrence" è chiaramente l'ampiezza del repertorio di capacità a cui oggi si può attingere.[107]

Un'ultima innovazione teorica introdotta dalla quinta ondata in relazione alla questione delle capacità riguarda il cosiddetto "paradosso capacitivo".[108] Tale concetto fa riferimento alle vulnerabilità che ogni attore che sviluppa maggiori capacità cyber introduce nel proprio "sistema", diventando nel contempo esponenzialmente più esposto a misure offensive contro le proprie reti fisiche e virtuali. Ciò rende la deterrenza

[107] King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica: RAND, 2018), 7. Il concetto di escalation laterale seppur innovativo ricorda sotto alcuni aspetti quello di escalation orizzontale, a sua volta un tema ricorrente. Si veda: Joshua M. Epstein, 'Horizontal Escalation: Sour Notes of a Recurrent Theme' International Security 8/3 (Winter 1983-1984), 19-31; F.C. Iklé, 'The Reagan Defense Program: A Focus on the Strategic Imperatives', *Strategic Review*, 10/2, 1982; Michael Fitzsimmons, 'Horizontal Escalation: An Asymmetric Approach to Russian Aggression?', *Strategic Studies Quarterly* 13/1 (Spring 2019), 95-133.
[108] Jacquelyn Schneider, *Digitally-Enabled Warfare: The Capability-Vulnerability Paradox* (Washington DC: Center for a New American Security, 2016).

potenzialmente molto più instabile e complessa, generando la possibilità per attori statali dotati di infrastrutture e sistemi di informazione meno sviluppati di utilizzare *proxies* per operazioni offensive negando poi all'avversario la possibilità di ritorsioni *in kind*, e dunque potenzialmente spingendo l'attore più forte verso un'escalation capacitiva, qualora non fosse in grado di operare efficacemente *cross-domain*.[109]

Anche per quanto concerne i meccanismi della deterrenza la quinta ondata ha introdotto innovazioni rilevanti. L'identificazione di nuovi meccanismi di funzionamento ha preso le mosse dalla difficoltà, riscontrata in molti studi, di adottare strategie di deterrenza fondate sui noti meccanismi della "punizione" e "negazione" nel cyberspazio, in particolare per la difficoltà di delineare in maniera chiara "linee rosse", "terreno di gioco" ed ambiti operativi.[110] Rifacendosi alla definizione di Glenn Snyder di "deterrenza ampia", mai sviluppata dalla letteratura precedente, sono stati identificati altri due meccanismi attraverso cui la deterrenza può operare: l'*entanglement* e le norme.[111] L'*entanglement* a volte chiamato "auto-deterrenza" e trattato come un caso di errata percezione,[112] si riferisce all'esistenza di interdipendenze che renderebbero l'attuazione di una minaccia deterrente estremamente costosa non solo per il bersaglio, ma anche per l'attore che la mette in atto.[113]

La percezione di tale evidenza ingenera auto-limitazione nell'attore che intende attuare la minaccia, trasformando la matrice costi/benefici da ante-impetum (pre-attacco)/post-impetum (post-attacco) ad una basata sulla gestione del rischio su base continuativa, facendolo desistere dall'agire.[114] Un esempio in tal senso può considerarsi la minaccia da parte della Cina di vendere considerevoli quantità di dollari detenuti nelle proprie riserve per far desistere gli USA dall'applicare misure commerciali dannose per il proprio sistema economico.[115]

---

[109] Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence,* 9; Ron Deibert, 'Circuits of Power: Security in the Internet Environment', in J. P. Singh and James N. Rosenau (eds.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (New York: SUNY Press, 2002), 115; Martin C. Libicki, *Cyber Deterrence and Cyberwar*, 36.

[110] Si veda ad esempio: Jim Chen, 'Cyber Deterrence by Engagement and Surprise', *PRISM* 7/2 (2017) THE FIFTH DOMAIN, 103 e Brandon Valeriano and Ryan C. Manness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Ben Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).

[111] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* 9-10.

[112] Jervis, 'Deterrence and Perception', 14.

[113] Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).

[114] Joseph S. Nye Jr., 'Deterrence and Dissuasion in Cyberspace', *International Security,* 41/3 (Winter 2016/17), 59.

[115] https://www.businessinsider.com/china-threat-to-sell-us-treasurys-would-backfire-catastrophically-2019-5?r=US&IR=T.

L'identificazione di tale meccanismo da parte degli studi della quinta ondata prende le mosse dal riscontro del notevole tasso di interdipendenza che caratterizza oggi le relazioni internazionali a ogni livello. Aree come la condivisione di informazioni in settori critici come la finanza e l'energia, lo sviluppo di mercati eterogenei e diversificati, comprendenti software e hardware provenienti da diversi sistemi economici, l'istituzione di catene di approvvigionamento globali, contribuiscono cumulativamente ad "intrappolare" potenziali avversari/competitori. In tale dominio umano/tecnologico in continua evoluzione secondo molti studiosi è impossibile per qualsiasi attore costruire una posizione di sicurezza indipendente.[116]

Un secondo meccanismo attraverso il quale, secondo gli studiosi della quinta ondata, la dissuasione potrebbe funzionare sono norme e tabù.[117] Nell'ambito cyber la differenza tra un'"arma offensiva" e un semplice "programma" può dipendere da una singola linea di codice, il che rende impossibile ogni forma di "controllo degli armamenti" o limitazioni allo sviluppo e possesso degli stessi.[118] In relazione a questo tipo di problemi alcuni studiosi hanno sottolineato come norme e tabù possano scoraggiare un corso d'azione di un avversario/competitore attraverso l'imposizione di costi reputazionali in grado di danneggiarne il soft power in maniera significativa.[119] A differenza dell'*entanglement*, tuttavia, perché questo meccanismo di deterrenza possa essere attivato, è fondamentale poter attribuire *ex post* ad un attore la responsabilità dell'atto che si intende scoraggiare.[120]

Anche in relazione alla concettualizzazione del processo della deterrenza la quinta ondata si è fino ad oggi dimostrata innovativa. Come precedentemente illustrato, la concettualizzazione del processo della deterrenza si è evoluta molto lentamente e, almeno fino alla "terza ondata" è stata pesantemente influenzata dal paradigma di processo psicologico basato sul potere consolidatosi nei primi anni di teorizzazione della

---

[116] Aaron Brantly, *Conceptualizing Cyber Deterrence by Entanglement* (April 05 2018). Si veda anche Stephen G. Brooks, *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict* (Princeton: Princeton University Press, 2006); Jonathan D. Caverley, 'United States Hegemony and the New Economics of Defense', *Security Studies*, 16/4 (October-December 2007), 598–614; Eugene Gholz, 'Globalization, Systems Integration, and the Future of Great Power War', *Security Studies*, 16/4 (October-December 2007), 615–636; Henry Farrell and Abraham L. Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44/1 (Summer 2019), 42-79.

[117] Brandon Valeriano and Ryan C. Manness, *Cyber War versus Cyber Reality,* 63.

[118] Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33/1 (2012), 148-170; Mariarosaria Taddeo, 'Deterrence and Norms to Foster Stability in Cyberspace', *Philosophy & Technology* 31/3 (September 2018), 323-329.

[119] Il più importante studio in materia è: Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons* (New York: Cambridge University Press, 2007).

[120] Joseph S. Nye Jr., 'Deterrence and Dissuasion in Cyberspace', 60-61.

deterrenza nucleare. I primi studi sulla deterrenza cyber, eredi della letteratura sulla 'information warfare' e 'cyberwar' degli anni 90[121] non si discostavano in maniera significativa dalla concettualizzazione dominante che vedeva la deterrenza come "prodotto" di un processo psicologico di percezione di potenza offensiva e difensiva derivante da significative capacità informative.[122] Allo stesso tempo tali studi non furono influenzati dalla quarta ondata.

In anni più recenti tuttavia sono apparse nella letteratura alcune concettualizzazioni estremamente innovative del processo della deterrenza. Esse affondano le radici nelle difficoltà e contraddizioni logiche in cui i primi studi sulla deterrenza cyber erano incorsi cercando di delinearne il processo attraverso quelle che potremmo chiamare le "categorie tradizionali". Tali difficoltà, ancora una volta, possono essere ricondotte alla peculiare natura del dominio cyber. Betz e Stevens ad esempio descrivono il conflitto nel cyberspazio come uno stato di costante "schermaglia", una incessante aggressione cibernetica, incluse attività di spionaggio, sabotaggio economico, furto di proprietà intellettuale, e disinformazione.[123] Erik Gartzke e Jon Lindsay si attestano su una posizione simile delineando un luogo di conflitto a "bassa intensità" permanente in cui è possibile operare in modo incrementale senza superare quella soglia di aggressività che potrebbe innescare un'*escalation*.[124] Una definizione esaustiva di quella che potremmo chiamare la "condizione di natura" del cyberspazio è stata fornita da Harknett e Fischerkeller. I due autori hanno sottolineato come gli attori nel cyberspazio si trovino in una condizione di ineludibile "contatto permanente e ubiquo" che a sua volta incoraggia strategie di "attacco persistente" a bassa intensità, molto più che di "moderazione operativa".[125] La sempre più diffusa consapevolezza di tale condizione (seppur non sempre esplicitata) può essere rinvenuta nei concetti di: "deterrenza cumulativa", "deterrenza seriale", e "deterrenza punteggiata". Il primo, la cui origine è da tracciarsi

---

[121] John Arquilla and David Ronfeldt, 'Cyber War is Coming!' *Comparative Strategy* 12/2 (1993), 65-141; James Der Derian, 'Cyber-Deterrence', *Wired* 2/9 (September 1994); Brian E. Fredericks, 'Information Warfare at the Crossroads', *Joint Force Quarterly*, no. 17 (Summer 1997), 98.

[122] Richard J. Harknett, 'Information Warfare and Deterrence', 98; John Arquilla and David Ronfeldt, The Advent of Net War (Santa Monica: RAND Corporation, 1996), 94.

[123] David Betz, & Tim Stevens, 'Analogical Reasoning and Cyber Security', 147–164.

[124] Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* 24/2 (2015), 316-348.

[125] Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation* (Alexandria: Institute for Defense Analysis, 2018), https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/ITSD/2018/D-9076.pdf. Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61/3 (2017), 381-393. Si veda anche: Richard Harknett and Emily Goldman, 'The Search for Cyber Fundamentals', *Journal of Information Warfare* 15/2 (2016), 81–88.

nell'esperienza israeliana, [126] concettualizza il processo della deterrenza come un processo lento, cumulativo di attrito derivante dalla combinazione di fattori psicologici e fisici. Si tratta di una concettualizzazione del processo della deterrenza come "inibitorio", non finalizzato ad evitare ogni episodio di scontro in una relazione conflittuale, ma piuttosto a circoscrivere e modellare una serie di conflitti di varia intensità in corso con una varietà di attori statali e sub-statali. In una tale visione, l'attuazione di una minaccia non rappresenta il preludio al fallimento di una strategia di deterrenza, ma piuttosto una parte inerente al mantenimento dell'efficacia della postura di deterrenza. L'attuazione coerente e ripetuta di minacce utilizzando tutti gli strumenti del potere di cui un attore dispone contribuisce infatti a "ricaricare la batteria" della deterrenza in modo continuativo, prevenendo in tal modo violazioni più ampie delle "regole del gioco". Tale paradigma parte dall'assunto che l'elemento psicologico, la percezione di forza, rimanga di per sé insufficiente come base di una minaccia deterrente credibile. Esso al contrario deve essere combinato con ripetuti usi della forza contro l'avversario/competitore per periodi di tempo protratti. L'uso della forza in questa prospettiva cerca di creare norme o mantenere le "regole del gioco" in uno sforzo continuo di influenzare il comportamento dell'avversario/competitore, piuttosto che impedire che singole azioni, seppur dannose, abbiano luogo.[127]

Una concettualizzazione simile del processo è stata elaborata da Patrick Morgan con il concetto di "deterrenza seriale" nel dominio cyber. In maniera simile al concetto di deterrenza cumulativa, tale paradigma parte dall'assunto dell'impossibilità di prevenire completamente gli attacchi informatici. Alla luce di tale evidenza, il processo di deterrenza sarebbe da intendersi come implicante una serie ripetuta di attuazione di minacce deterrenti per un lungo periodo di tempo in risposta a "violazioni" di entità relativamente circoscritta, per indurre nell'avversario/competitore un certo livello di cautela circa l'opportunità di attuare attacchi di entità maggiore.[128]

---

[126] Uri Bar-Joseph, 'Variations on a theme: The Conceptualization of Deterrence in Israeli Strategic Thinking' Security Studies 7/3 (1998), 145-181; Niccolò Petrelli, *Israel, Strategic Culture and the Conflict with Hamas: Adaptation and Military Effectiveness* (London: Routledge, 2018), 23-25.

[127] Uri Tor 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40/1-2 (2017), 96, 107.

[128] Patrick M. Morgan, 'Deterrence and System Management: The Case of North Korea', *Conflict Management and Peace Science* 23/2 *SPECIAL ISSUE: Deterrence* (Summer 2006), 121-138; Patrick M. Morgan, 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in John D. Steinbruner et al. (eds.) *Proceedings of a Workshop on Deterring Cyberspace*, 51. Si veda anche: Amir Lupovici, 'Cyber Warfare and Deterrence', *INSS Military and Strategic Affairs* 3/3 (December 2011), 49-61.

Da ultimo, il concetto di "deterrenza punteggiata", è stato elaborato da Luka Kello, che lo definisce come "una serie di azioni che generano un effetto cumulativo, piuttosto che una risposta *tit for tat*". La "deterrenza punteggiata" parte all'assunto che nel cyberspazio la deterrenza "assoluta", ovvero la completa astensione del "bersaglio" da comportamenti aggressivi (come nella deterrenza nucleare) sia impossibile dal momento che il l'attività offensiva persistente. Il processo della deterrenza si configura dunque come uno schema graduato in cui minacce e impiego della forza sono comminate nel tempo ed in momenti specificamente scelti dall'attore che attua la strategia di deterrenza sulla base di una logica di punizione più flessibile che faccia riferimento non a singole azioni ma ad un insieme, perseguendo effetti cumulativi.[129]

Conclusioni

Questo studio ha esaminato l'evoluzione della teoria della deterrenza dalla formulazione originaria del concetto sino alle più recenti al fine di identificare i cambiamenti intervenuti nel fenomeno. Due conclusioni possono trarsi circa la sua traiettoria evolutiva. Sotto il profilo ontologico, la ricerca rivela una transizione della deterrenza da fenomeno relativamente lineare a complesso, la cui struttura e modello di funzionamento possono essere assimilati ad un *network*. In altri termini, da processo lineare di comunicazione di minacce progressivamente sempre più intense finalizzato a condizionare il calcolo strategico dell'avversario generando un effetto psicologico, la deterrenza si è trasformata in un processo non-lineare di formulazione di minacce ed uso della violenza, suscettibili di variare verticalmente e orizzontalmente, finalizzato a obbligare e condizionare il comportamento di un avversario/competitore attraverso effetti psicologici e fisici. Sotto il profilo concettuale la conclusione di questo studio è che attraverso le varie ondate di teoria, il termine deterrenza ha cambiato significato, fondendosi progressivamente con il concetto contiguo di *compellenza*.

Durante la Guerra Fredda, lo stratega Hermann Kahn equiparò in un noto studio il funzionamento della deterrenza ad una scala, i cui pioli rappresentavano i possibili livelli nella minaccia dell'uso della forza a fini coercitivi. Tale modello ha esercitato una notevole influenza ed ha rappresentato per molti anni il paradigma concettuale (a volte inconscio) attraverso cui studiosi, politici, funzionari pubblici pensavano la deterrenza ed il suo funzionamento. Esso appare tuttavia oggi drammaticamente inadeguato a rappresentare la natura e quelli che potremmo definire i possibili "percorsi", del fenomeno.

[129] Lukas Kello, *The Virtual Weapon and International Order* (New Haven: Yale UP, 2018), 197.

Da questo elaborato emerge come la più moderna teoria della deterrenza abbia evidenziato percorsi di funzionamento multipli del fenomeno, sia orizzontali che verticali. Una metafora più appropriata per pensarne il funzionamento della deterrenza in senso ampio appare dunque quella di una rete di percorsi trasversali ed intersecanti assimilabili ad un *network*. In tale modello, ad una minaccia in uno specifico dominio e/o fondata su un determinato meccanismo è possibile rispondere in un dominio alternativo, con un tipo di capacità differente attivando un meccanismo di altro tipo. Tale sempre più diffusa consapevolezza si è tradotta a livello concettuale in quanto accennato pocanzi: una progressiva fusione della nozione di deterrenza con quella di compellenza. Quest'ultima può essere definita un'altra strategia coercitiva mirante a costringere l'obiettivo a intraprendere un'azione o a sospenderne una già in corso. In altre parole, come sottolineato da Lawrence Freedman, la compellenza riguarda la modifica del comportamento di un avversario/competitore più che il condizionamento del suo calcolo strategico.[130] La convergenza tra il concetto di compellenza e nozioni recentemente introdotte nella teoria della deterrenza e qui discusse, come "deterrenza cumulativa", deterrenza "tailored" deterrenza "cross-domain" appare evidente dall'esame qui condotto. Tradizionalmente la differenza tra deterrenza e compellenza si ritiene riguardi l'approccio allo status quo (difensivo per la deterrenza e offensivo per la compellenza), e al tempo e l'azione (passivo per la deterrenza e attivo per la compellenza). Al contrario le formulazioni del concetto di deterrenza avanzate più recentemente, nella quarta e quinta ondata, appaiono caratterizzate da aspetti per molto tempo considerati propri della compellenza. Esse prevedono infatti una condotta strategica più attiva, volta a influenzare in senso sia positivo che negativo il calcolo strategico e comportamento dell'avversario/competitore attraverso un'iniziativa permanente e costante.

Quali possono essere considerate le implicazioni pratiche di quanto sopra? In altre parole, quanto spazio esiste oggi per le strategie di deterrenza, soprattutto nel quadro delle "grandi strategie" degli attori globali? Combinando le conclusioni di questo elaborato con una breve analisi di quelli che possono considerarsi i due trend fondamentali che plasmeranno il sistema internazionale nel prossimo futuro è possibile fornire una risposta di massima.

Il primo trend è il ritorno della competizione internazionale, in particolare tra USA da una parte e Cina e Russia dall'altra ma anche, seppur in maniera minore, tra UE e Cina e UE e

[130] Lawrence Freedman, *Deterrence* (Cambridge: Polity, 2004).

Russia. La "competizione" in ambito di relazioni internazionali coinvolge due o più attori che si contendono "beni" relativamente scarsi, il cui ottenimento può portare una delle parti ad aumentare il proprio potere o influenza rispetto all'altra (o altre).[131] In sostanza, quindi, la "competizione" implica il tentativo di ottenere risorse e relazioni che sono "voluti" anche da altri attori, quali essi siano, sicurezza, ricchezza, influenza e status, in misura maggiore rispetto ai "concorrenti".[132] In un tale sistema di relazioni le strategie di deterrenza rimarranno in una certa misura indispensabili al fine di controllare processi di escalation, in particolar modo nella competizione in ambito militare, nel quadro delle cosiddette *grey-area operations*.[133]

Il secondo trend, come sottolineato nell'ultimo rapporto Alternative Futures del National Intelligence Council USA, riguarda le basi del potere nel sistema internazionale, le quali con buona probabilità nei prossimi 20 anni cambieranno. Fattori materiali, come le dimensioni dell'economia, delle forze armate e della popolazione di una nazione, nonché il suo livello di sviluppo tecnologico, continueranno a fornire le basi necessarie per esercitare il potere, ma saranno di per sé sempre meno sufficienti a produrre risultati favorevoli nella condotta della politica estera. In un mondo interdipendente ed iperconnesso, incideranno sempre più sulla capacità di esercitare potere nel sistema internazionale la capacità di sviluppare e applicare tecnologie innovative, nonché di definirne gli standard di impiego in ambito internazionale, il capitale umano, la capacità di generare, acquisire e proteggere informazioni e posizione all'interno dei sempre più densi network internazionali. Anche la capacità di attrazione delle istituzioni di intrattenimento, sportive, turistiche e educative di un paese rimarranno importanti fattori alla base della sua capacità di produrre esiti favorevoli. Con l'intensificarsi di sfide globali come eventi meteorologici estremi e crisi umanitarie, la resilienza interna agli shock e ai cambiamenti sistemici diventerà un elemento essenziale alla base del potere.[134] Contrariamente al primo trend, questo secondo sembra presagire una minore futura rilevanza delle strategie di deterrenza, considerato che le basi del potere si sposteranno verso una combinazione di fattori materiali ed immateriali che ne renderà più complicate

[131] Howard J. Shatz, *Economic Competition in the 21st Century* (Santa Monica: RAND, 2020), 3; Michael J. Mazarr et al., *Understanding the Emerging Era of International Competition* (Santa Monica: RAND, 2018), 4.
[132] Raymond Mack, 'The Components of Social Conflict', *Social Problems* 22/4 (Spring 1965), 388-397.
[133] Anthony H. Cordesman with the assistance of Grace Hwang, *U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy* (Washington DC: Center for Strategic and International Studies, 2020).
[134] National Intelligence Council, *Global Trends 2040, Navigating a More Contested World* (Washington DC: National Intelligence Council, 2021).

elaborazione ed esecuzione. Alla luce della maggiore complessità del fenomeno della deterrenza illustrata in questo studio, sembrerebbe dunque possibile ipotizzare che nel prossimo futuro essa sarà relegata ad un ruolo minore, circoscritto all'ambito militare. In realtà la risposta a questo quesito è più sfumata.

La deterrenza non solo continuerà ad occupare un ruolo nel quadro della politica estera degli attori globali in campo militare (nucleare e convenzionale), ma molto probabilmente sarà presente anche in altri ambiti, si pensi ad esempio alla questione dei network (commerciali, infrastrutturali ecc..) ed alla possibilità di sviluppare forme di deterrenza basate sul *gatekeeping*, ovvero sulla minaccia di estromissione (o declassamento) di un attore dal network stesso.[135] La deterrenza assolverà dunque il ruolo sia di strumento di gestione dei conflitti, sia di strumento di competizione. La differenza fondamentale rispetto al passato è il ruolo che essa andrà ad occupare.

Per quanto il concetto sia antico, la deterrenza non è stata impiegata come strumento politico in maniera consapevole e strutturata prima del periodo immediatamente successivo alla Seconda Guerra Mondiale, più o meno in coincidenza con il suo sviluppo teorico. Tra il 1945 e il 1991, durante la Guerra Fredda, la deterrenza ha rappresentato una componente chiave della politica nazionale di USA e URSS nonché di altre potenze, in ambito militare e particolarmente in quello nucleare. Ciò ha prodotto una generalizzata tendenza ad attribuire, seppur a volte inconsapevolmente, una "naturale" centralità alla deterrenza (qualora presente nella politica estera di un attore). Al contrario, in futuro è probabile che essa avrà un ambito di applicazione più ampio, ovvero in campi molto diversi da quello in cui la sua teorizzazione ha avuto origine, ma il suo ruolo sarà più circoscritto, rappresenterà una strategia "di teatro", "di dominio", una "tattica" nel quadro di politiche estera volte a sintetizzare cooperazione e competizione.

Bibliografia

Abrahms, Max, and Philip B.K. Potter, "Explaining Terrorism: Leadership Deficits and Militant Group Tactics," *International Organization*, Vol. 69, No. 2 (Spring 2015), 311-342.
Acton, James M., 'Extended Deterrence and Communicating Resolve' *Strategic Insights*, 8/5 (December 2009).
Adamsky, Dmitry (Dima), 'From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force', *Security Studies* 26/1 (2016), 157-184.
Adamsky, Dmitry (Dima), 'From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies*, 41/1-2 (2018), 33-60.

[135] Sul concetto di gatekeeping all'interno dei network si veda: Joshua Cooper Ramo, *The Seventh Sense: Power, Fortune, and Survival in the Age of Networks* (New York: Little, Brown and Company, 2016).

Adler, Emanuel, 'The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control', *International Organization* 46/1 (1992).
Arquilla, John, and David Ronfeldt, 'Cyber War is Coming!' *Comparative Strategy* 12/2 (1993), 65-141.
Arquilla, John, and David Ronfeldt, The Advent of Net War (Santa Monica: RAND Corporation, 1996).
Bar-Joseph, Uri, 'Israel's Military Intelligence Performance in the Second Lebanon War', *International Journal of Intelligence and CounterIntelligence*, 20/3 (2007), 583-601.
Bar-Joseph, Uri, 'Variations on a theme: The Conceptualization of Deterrence in Israeli Strategic Thinking' Security Studies 7/3 (1998), 145-181.
Baylis, John, 'The Concept of 'Tailored Deterrence' in the 'Second Nuclear Age'', *St Antony's International Review*, 4/2 (February 2009), 8-23.
Beniger, James R., *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge: Harvard University Press, 1986).
Berkowitz, Bruce D., 'Warfare in the Information Age', in John Arquilla and David F. Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997), 183-184
Betts, Richard, 'Conventional Deterrence', *World Politics* 37/2 (January 1985), 153-79.
Betz, David, & Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue,* 44/*2* (2013), 147–164.
Borghard, Erica D., and Shawn W. Lonergan, 'Can States Calculate the Risks of Using Cyber Proxies?', *Orbis* 60/3 (2016), 395-416.
Bowen, Wyn Q., 'Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism', *Contemporary Security Policy*, 25/1 (April 2004).
Brands, Hal, *American Grand Strategy in the Age of Trump* (Washington DC: Brookings Institution Press, 2018).
Brantly, Aaron F., 'Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace', *Intelligence and National Security* 31/5 (2015), 674-685.
Brantly, Aaron F., 'Ambiguous Deterrence', *The Cyber Defense Review*, January 23 2016.
Brantly, Aaron F., 'The Cyber Deterrence Problem' in *The 10th International Conference on Cyber Conflict* (Tallinn: NATO Cyber Defense Center of Excellence, 2018), 31–54.
Brodie, Bernard (Ed.) *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946).
Brodie, Bernard, 'Why Were We So (Strategically) Wrong?', *Foreign Policy* No. 5 (Winter, 1971-1972), 151-161.
Brodie, Bernard, *The Anatomy of Deterrence* (Santa Monica: RAND, 1958), 1-5;
Brooks, Stephen G., and William C. Wohlforth, 'The Rise and Fall of the Great Powers in the Twenty-first Century: China's Rise and the Fate of America's Global Position', *International Security* 40/3 (Winter 2015/16), 7-53.
Brooks, Stephen G., *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict* (Princeton: Princeton University Press, 2006).
Buchanan, Ben, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard UP, 2020).
Buchanan, Ben, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).
Caverley, Jonathan D., 'United States Hegemony and the New Economics of Defense', *Security Studies*, 16/4 (October-December 2007), 598–614.
Chadwick, Andrew, & Philip Howard (Eds.), *Routledge Handbook of Internet Politics* (London: Routledge 2009).
Chen, Jim, 'Cyber Deterrence by Engagement and Surprise', *PRISM* 7/2 (2017) THE FIFTH DOMAIN.
Clark, Bruce H., and David B. Montgomery, 'Deterrence, Reputations, and Competitive Cognition', *Management Science* 44/1 (January 1998), 62-82.
Cordesman, Anthony H. with the assistance of Grace Hwang, *U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy* (Washington DC: Center for Strategic and International Studies, 2020).
Cordesman, Antony, & Justin Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Washington DC: CSIS, 2002).
Cote', Owen, "Assessing the Undersea Balance between the United States and China," Thomas G. Mahnken (ed.), *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Palo Alto: Stanford University Press, 2012), 184-205.
Crawford, Timothy W., 'Pivotal Deterrence and the Kosovo War: Why the Holbrooke Agreement Failed', *Political Science Quarterly* 116/4 (2002), 499-523

Crawford, Timothy W., *Pivotal Deterrence: Third-Party Statecraft and the Pursuit of Peace* (Ithaca: Cornell University Press, 2004).
Dalsjö, Robert, Christofer Berglund, Michael Jonsson, *Bursting the Bubble: Russian A2/AD in the Baltic Sea Region:Capabilities, Countermeasures, and Implications* (Stockholm: FOI, 2019).
Davis, Paul K., Brian Michael Jenkins, 'A System Approach to Deterring and Influencing Terrorists', *Conflict Management and Peace Science* 21/1 (2004), 3-15.
Davis, Paul K., Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism A Component in the War on al Qaeda* (Santa Monica: RAND, 2002).
Deibert, Ron, 'Circuits of Power: Security in the Internet Environment', in J. P. Singh and James N. Rosenau (eds.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (New York: SUNY Press, 2002).
Der Derian, James, 'Cyber-Deterrence', *Wired* 2/9 (September 1994).
Dunn, Lewis A., 'Can al Qaeda Be Deterred from Using Nuclear Weapons?', Occasional Paper 3, Center for the Study of Weapons of Mass Destruction (Washington DC: National Defense University Press, July 2005).
Dutta, Prajit K., *Strategies and Games: Theory and Practice* (Cambridge: The MIT Press, 1999).
Ellsberg, Daniel, *The Theory and Practice of Blackmail* (Santa Monica: RAND Corporation, 1968).
Epstein, Joshua M., 'Horizontal Escalation: Sour Notes of a Recurrent Theme' *International Security* 8/3 (Winter 1983-1984), 19-31
Erickson, Andrew S., 'Deterrence by Denial: How to Prevent China From Using Force', *the National Interest*, December, 16, 2013.
Evron, Yair, *War and Intervention in Lebanon: The Israeli-Syrian Deterrence Dialogue* (London: Routledge, 1987).
Farrell, Henry, and Abraham L. Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44/1 (Summer 2019), 42-79.
Fischerkeller, Michael P., and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation* (Alexandria: Institute for Defense Analysis, 2018),
Fischerkeller, Michael P., and Richard J. Harknett,, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61/3 (2017), 381-393.
Fitzsimmons, Michael, 'Horizontal Escalation: An Asymmetric Approach to Russian Aggression?', *Strategic Studies Quarterly* 13/1 (Spring 2019), 95-133.
Fredericks, Brian, 'Information Warfare at the Crossroads', *Joint Force Quarterly*, no. 17 (Summer 1997).
Freedman, Lawrence, *Deterrence* (Cambridge: Polity Press, 2004).
Garfinkle, Adam, 'Does Nuclear Deterrence Apply in the Age of Terrorism?', *Footnotes: The Newsletter of FPRI's Wachman Center* 14/10 (May 2009).
Gartzke, Erik, and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* 24/2 (2015), 316-348.
Garztke, Eric, and Jon Lindsay, "Cross-Domain Deterrence: Strategy in an Era of Complexity," working paper, University of California Institute on Global Conflict and Cooperation (IGCC), 15 July 2014
George, Alexander L., & Andrew Bennet, *Case Studies and Theory Development in the Social Sciences* (Cambridge: the MIT Press, 2005).
George, Alexander L., 'The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries', *Comparative Strategy* 22/5 (December 2003).
George, Alexander L., and Richard Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974).
Gerson, Michael & Daniel Whiteneck, *Deterrence and Influence: The Navy's Role in Preventing War* (Arlington: Center for Naval Analyses, 2009)
Gholz, Eugene, 'Globalization, Systems Integration, and the Future of Great Power War', *Security Studies*, 16/4 (October-December 2007), 615–636.
Glaser, Charles L., Andrew H. Kydd, Mark L. Haas, John M. Owen IV and Sebastian Rosato, 'Correspondence: Can Great Powers Discern Intentions?', *International Security* 40/3 (Winter 2015/16), 197-215.
Glaser, Charles, 'Deterrence of Cyber Attacks and U.S. National Security', GW-CSPRI no. 5 (2011).
Goldman, Emily O. (ed.), *National Security in the Information Age* (New York: Routledge, 2004), 3, 210-213.
Tabansky, Lior, 'Basic Concepts in Cyber Warfare', *INSS Military and Strategic Affairs* 3/1 (2011), 75-92.
Gompert, David and Martin Libicki, 'Waging Cyber War the American Way', *Survival* 57/4 (2015).
Gray, Colin S., 'Gaining Compliance: The Theory of Deterrence and its Modern Application', *Comparative Strategy*, 29/3 (2010), 278-283.
Gray, Colin S., 'Nuclear Strategy: The Case for a Theory of Victory', *International Security* 4/1 (Summer, 1979), 54-87.
Gray, Colin S., 'The Reformation of Deterrence: Moving On', *Comparative Strategy* 22/5 (December 2003), 429-461.

Gray, Colin S., 'What Rand Hath Wrought', *Foreign Policy* No. 4 (Autumn, 1971), 111-129.
Gray, Colin S., *Maintaining Effective Deterrence* (Carlisle: US Army War College, August 2003), 7.
Gray, Colin S., *Strategy and Defence Planning: Meeting the Challenge of Uncertainty* (Oxford: Oxford University Press, 2016).
Gray, Colin S., *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2012).
Green, Brendan Rittenhouse & Austin Long, *The Role of Clandestine Capabilities in Deterrence: Theory and Practice* (U.S. Naval Postgraduate School Project on Advanced Systems and Concepts for Countering WMD Final Report September 2017).
Gross Stein, Janice, 'Deterrence and Learning in an Enduring Rivalry: Egypt and Israel 1948-73', *Security Studies* 6/1 (1996), 104-152.
Grygiel, Jakub, and A Mitchell Wess, 'Limited War is Back', *The National Interest*, No. 135 (August 2014).
Guzansky, Yoel, 'Lines in the Sand: the Use and Misuse of Red Lines', *Defense & Security Analysis* 31/2 (2015), 90-98.
Hannan, Michael J., *Operational Net Assessment: A Framework for Social Network Analysis and Requirements for Critical Debate* (Monterey: Naval Postgraduate School, 2005).
Harknett, Richard J., 'Information Warfare and Deterrence', *Parameters* 26/3 (1996), 93-107.
Harknett, Richard, and Emily Goldman, 'The Search for Cyber Fundamentals', *Journal of Information Warfare* 15/2 (2016), 81–88.
Harvey, Frank P., 'Rigor Mortis, or Rigor, More Tests: Necessity, Sufficiency, and Deterrence Logic', *International Studies Quarterly* 42 (December 1998), 675-707.
Helmer, Olaf, *Deterrence* (Santa Monica: RAND Corporation, 1957).
Henry, Shawn and Aaron F. Brantly, 'Countering the Cyber Threat', *The Cyber Defense Review* 3/1 (Spring 2018), 47-56.
Hoffman, Bruce & Marc Sageman, 'Does Osama Still Call the Shots? Debating the Containment of Al Qaeda's Leadership', *Foreign Affairs*, 87/4 (July/August 2008), 163–166.
Huntington, Samuel P., 'Conventional Deterrence and Conventional Retaliation in Europe', *International Security* 8/3 (Winter 1983-1984), 32-56.
Huth, Paul and Bruce Russett, 'General Deterrence Between Enduring-Rivals: Testing Three Competing Models', *American Political Science Review* 87/1 (1993), 61-73.
Huth, Paul, 'Deterrence and International Conflict: Empirical Findings and Theoretical Debates', *Annual Review of Political Science*, 2 (1999), 25-48.
Huth, Paul, and Bruce Russett, 'Testing Deterrence Theory: Rigor Makes a Difference', *World Politics* 42/4 (July 1990), 466-501.
Huth, Paul, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press 1988).
Iklé, F.C., 'The Reagan Defense Program: A Focus on the Strategic Imperatives', *Strategic Review*, 10/2, (1982).
Jackson, Van, 'Beyond Tailoring: North Korea and the Promise of Managed Deterrence', *Contemporary Security Policy* 33/2 (2012), 289-310.
Jervis, Robert, 'Deterrence and Perception', *International Security* 7/3 (Winter, 1982-1983), 3-30; Richard Lebow, Richard Ned, and Janice Gross Stein, 'Rational Deterrence Theory: I Think, Therefore I Deter', World Politics 41/2 (January 1989), 208-224.
Jervis, Robert, 'Deterrence Theory Revisited', and 'Rational Deterrence: Theory and Evidence', World Politics 42/2 (1989), 183-207.
Jervis, Robert, 'Review Article: Deterrence Theory Revisited', *World Politics* 31/2 (January 1979), 289-324.
Knopf, Jeffrey W., 'The Fourth Wave in Deterrence Research', *Contemporary Security Policy*, 31/1 (2010), 1-33.
Jervis, Robert, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare*, 15/2 (2016).
Jervis, Robert, 'The Confrontation between Iraq and the US: Implications for the Theory and Practice of Deterrence', *European Journal of International Relations*, 9/2 (June 2003).
Jervis, Robert, Richard Ned Lebow, and Janice Gross Stein, eds., *Psychology and Deterrence* (Baltimore: Johns Hopkins University Press, 1985).
Johnston, Patrick B., "Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns," *International Security*, Vol. 36, No. 4 (Spring 2012), 47-79.
Jordan, Amos A. Jr., 'Basic Deterrence and the New Balance of Power', *Journal of International Affairs* 14/1 (1960), 49-60.
Jordan, Jenna, 'Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes', *International Security* 38/4 (Spring 2014), 7–38.
Kahn, Herman, *On Escalation: Metaphors and Scenarios* (Westport: Praeger, 1965).
Kahn, Herman, *On Thermonuclear War* (Princeton: Princeton University Press, 1960).

Kahn, Herman, *Thinking about the Unthinkable* (New York: Horizon Press, 1962).
Kamp, Karl-Heinz, and David S. Yost (eds.), *NATO and 21st Century Deterrence*, NDC Forum Paper 8 (Rome: NATO Defense College, May 2009).
Kaplan, Morton A., *Some Problems in the Strategic Analysis of International Politics* (Princeton: Center for International Studies, 1959)
Karber, Philip, Net Assessment *for SecDef. Future Implications from Early Formulations* (Washington DC: Potomac Foundation, 2015).
Kaufmann, William W. (ed.), *Military Policy and National Security* (Princeton: Princeton University Press, 1956).
Kaufmann, William W., *The Evolution of Deterrence 1945–1958* (Santa Monica: RAND Corporation, 1958).
Kello, Lukas, *The Virtual Weapon and International Order* (New Haven: Yale UP, 2018).
Kenyon, Ian R., and John Simpson (eds.), *Deterrence and the New Global Security Environment* (London: Routledge, 2006).
Keohane, Robert O., and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).
Kratochwil, Friedrich, *International Order and Foreign Policy* (Boulder: Westview Press, 1978), 155-156.
Krepinevich, Andrew, Barry Watt and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessment, 2003).
Kugler, Richard L., 'Deterrence of Cyber Attacks', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington DC: National Defense University Press, 2009).
Larkin, Sean P., *Cracks in the New Jar: The Limits of Tailored Deterrence* (Carlisle: US Army War College, 2011).
Lebow, Richard Ned and Janice Gross Stein, 'Beyond Deterrence', *Journal of Social Issues* 43/4 (1987), 5-71.
Lebow, Richard Ned and Janice Gross Stein, 'The Elusive Variable', *World Politics* 42/3 (1990), 336-369.
Lebow, Richard Ned, and Janice Gross Stein, 'Beyond Deterrence'. *Journal of Social Issues* 43/4 (1987), 5-71.
Lebow, Richard Ned, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981).
Lepgold, Joseph, 'Hypotheses on Vulnerability: Are Terrorists and Drug Dealers Coercable?', in Lawrence Freedman (ed.), *Strategic Coercion: Concepts and Cases* (New York: Oxford University Press, 1998).
Levy, Jack S., 'Prospect Theory and International Relations: Theoretical Applications and Analytical Problems', *Political Psychology* 13/2 (1992), 283-310.
Levy, Jack S., 'When Do Deterrent Threats Work?', *British Journal of Political Science* 18/4 (October 1988), 486.
Levy, Jack, 'Learning and Foreign Policy: Sweeping a Conceptual Minefield', *International Organization* 48/2 (1994), 279-312.
Libicki, Martin C., 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly* 12/4 (Winter 2018), 46.
Libicki, Martin C., 'The Strategic Uses of Ambiguity in Cyberspace', *INSS Military and Strategic Affairs*, 3/3 (December 2011), 3-10.
Libicki, Martin C., *Conquest in Cyberspace* (Cambridge, Cambridge University Press, 2007).
Libicki, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009).
Libro Bianco per la Sicurezza Internazionale e la Difesa (Roma: Ministero della Difesa, 2015).
Long, Austin, 'Deterrence: The State of the Field', *NYU Journal of International Law and Politics* 47/2 (Winter 2015), 357-377.
Long, Austin, *Deterrence Lessons from Six Decades of RAND Research* (Santa Monica: RAND Corporation, 2012).
Long, Jerry Mark & Alex Wilner, 'Delegitimizing al-Qaida: Defeating an 'Army Whose Men Love Death', *International Security* 39/1 (Summer 2014), 126-164.
Lupovici, Amir, 'Cyber Warfare and Deterrence', *INSS Military and Strategic Affairs* 3/3 (December 2011), 49-61.
Lupovici, Amir, 'The Emerging Fourth Wave of Deterrence Theory-Toward a New Research Agenda', *International Studies Quarterly* 54/3 (September 2010), 705-732.
M. Elaine Bunn, 'Can Deterrence be Tailored?', *Strategic Forum* no. 255 (January 2007).
Mack, Raymond M, 'The Components of Social Conflict', *Social Problems* 22/4 (Spring 1965), 388-397.
Mallory, King, *New Challenges in Cross-Domain Deterrence* (Santa Monica: RAND, 2018).
Mandel, Robert, *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks* (Washington DC: Georgetown University Press, 2017).
Manzo, Vincent, 'Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?', *Strategic Forum*, no. 272 (December 2011).
Mazarr, Michael J., et al., *Understanding the Emerging Era of International Competition* (Santa Monica: RAND, 2018).

McCanles, Michael, 'Machiavelli and the Paradoxes of Deterrence', Diacritics 14/2 (Summer 1984), 11-19.
Mearsheimer, John J., *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983).
Millett, Allan R., Williamson Murray, and Kenneth H. Watman, 'The Effectiveness of Military Organizations', in Allan R. Millet and Williamson Murray, *Military Effectiveness: Volume 1: The First World War* (Cambridge: Cambridge University Press, 2010, New Edition), 1-30.
Mishal, Shaul & Maoz Rosenthal, 'Al Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations' *Studies in Conflict & Terrorism* 28/4 (2005), 275-293.
Mokyr, Joel, *The Gifts of Athena: Historical Origins of the Knowledge Economy* (Princeton: Princeton University Press, 2002).
Morgan, Patrick M., 'Deterrence and System Management: The Case of North Korea', *Conflict Management and Peace Science* 23/2 *SPECIAL ISSUE: Deterrence* (Summer 2006), 121-138.
Morgan, Patrick M., 'The Concept of Deterrence and Deterrence Theory', *Oxford Research Encyclopedia of Politics* (Oxford: Oxford UP, 2017).
Morgan, Patrick M., *Deterrence Now* (Cambridge: Cambridge University Press, 2003).
Morgan, Patrick, 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in John D. Steinbruner et al. (eds.) *Proceedings of a Workshop on Deterring Cyberspace: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010).
Mueller, Karl P., 'Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century', *Strategic Studies Quarterly* 12/4 (Winter 2018), 76-93.
Mueller, Richard, 'The Origins of Mad: A Short History of City-Busting', in Henry D. Sokolski (ed.) *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice* (Carlisle: Strategic Studies Institute, US Army War College 2004).
Murray, William S., 'A Will to Measure', *Parameters* 31/3 (Autumn 2001), 134-147.
Murray, Williamson, 'Operational Net Assessment Or, Preparing to Lose the Next War', in NIDS International Symposium on Security Affairs, *Strategic Management of Military Capabilities: Seeking Ways to Foster Military Innovation* (Tokyo: National Institute for Defense Studies, 2013), 43-55
Mushen, Emily, and Jonathan Schroden, Are *We Winning? A Brief History of Military Operations Assessment* (Arlington: Center for Naval Analyses, 2014).
Narang, Vipin, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton: Princeton University Press, 2014).
Nincic, Miroslav, Getting What You Want: Positive Inducement in International Relations, *International Security* 35/1 (Summer 2010), 138-183.
North, Douglass C., *Institutions, Institutional Change, and Economic Performance* (New York: Cambridge University Press, 1990).
Nye, Joseph S. Jr., 'Deterrence and Dissuasion in Cyberspace', *International Security,* 41/3 (Winter 2016/17).
Nye, Joseph, 'Nuclear Learning and the US-Soviet Security Regime', *International Organization* 41/3 (1987), 371-402.
Overy, R.J. 'Air Power and the Origins of Deterrence Theory before 1939', *Journal of Strategic Studies* 15/1 (1992), 74-76.
Paul, T.V., 'Complex Deterrence: An Introduction' in T.V. Paul, Patrick Morgan, and James Wirtz (eds.), *Complex Deterrence* (Chicago: University of Chicago Press, 2009).
Payne, Keith B., 'Maintaining Flexible and Resilient Capabilities for Nuclear Deterrence', *Strategic Studies Quarterly* 5/2 (Summer 2011), 13-29.
Petrelli, Niccolò, *Israel, Strategic Culture and the Conflict with Hamas: Adaptation and Military Effectiveness* (London: Routledge, 2018).
Petrelli, Niccolò, *Net Assessment and Grand Strategy: Theory for Practice* (manoscritto non pubblicato).
Pifer, Stephen, 'Dealing with Russia and Drawing Red Lines', *Order from Chaos Blog*, March, 10, 2017.
Post, Jerrold M., 'Deterrence in an Age of Asymmetric Rivals', in Stanley A. Renshon and Peter Suedfeld (eds.), *Understanding the Bush Doctrine* (New York: Routledge, 2007).
Prior, Tim, 'Resilience: The 'Fifth Wave' in the Evolution of Deterrence', in Oliver Thränert, Martin Zapfe (eds.) *Strategic Trends 2018: Key Developments in Global Affairs* (Zurich: Center for Security Studies ETH Zurich, 2018), 63-79.
Quackenbush, Stephen L., 'Deterrence theory: Where Do We Stand?', *Review of International Studies*, 37 (2011), 750.
Quester, George H., *Deterrence before Hiroshima. The Airpower Background of Modern Strategy* (New York: John Wiley & Sons, 1966).
Quinlan, Michael, 'Deterrence and Deterrability', *Contemporary Security Policy*, 25/1 (April 2004).
Raser, John, 'Deterrence Research: Past Progress and Future Needs', *Journal of Peace Research* 3/4 (1966), 297-327.

Rid, Thomas and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38/1-2 (2015), 4-37.
Roberts, Brad, 'Deterring Terrorism: Terrorist Campaigns and Prolonged Wars of Mutual Coercion', in Institute for Defense Analyses, *Deterring Terrorism: Exploring Theory and Methods* (Alexandria: Institute for Defense Analyses, August 2002).
Roberts, Brad, *Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction* (Alexandria: Institute for Defense Analyses, June 2007).
Rosato, Sebastian, 'The Inscrutable Intentions of Great Powers' *International Security* 39/3 (Winter 2014/15) 48-88.
Schelling, Thomas C., *Arms and Influence* (New Haven: Yale University Press, 1966).
Schneider, Jacquelyn, *Digitally-Enabled Warfare: The Capability-Vulnerability Paradox* (Washington DC: Center for a New American Security, 2016).
Schwartz, David N., 'The Role of Deterrence in NATO Defense Strategy: Implications for Doctrine and Posture', *World Politics* 28/1 (Oct., 1975), 118-133;
Shatz, Howard J., *Economic Competition in the 21st Century* (Santa Monica: RAND, 2020).
Shimshoni, Johnathan, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988).
Smeets, Max and Herbert S. Lin, 'Offensive Cyber Capabilities: To What Ends?', in Tomáš Minárik, Raik Jakschis, and Lauri Lindstrom (eds.), *2018 10th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2018).
Smelser, Neil J., and Faith Mitchell (eds.), *Discouraging Terrorism: Some Implications of 9/11*, National Research Council study (Washington DC: National Academies Press, 2002).
Smith, Derek D., *Deterring America: Rogue States and the Proliferation of Weapons of Mass Destruction* (New York: Cambridge University Press, 2006).
Snyder, Glenn H., 'Deterrence and Power', *The Journal of Conflict Resolution* 4/2 (June 1960), 163-178
Snyder, Glenn H., *Deterrence and Defense* (Princeton: Princeton University Press, 1961).
Sobelman, Daniel, 'Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–16', *International Security* 41/3 (Winter 2016/17), 151-196.
Steiner, Barry, *Bernard Brodie and the Foundation of American Nuclear Strategy* (Lawrence: University Press of Kansas, 1991).
Stern, Paul C., et al. (eds.), *Perspectives on Deterrence* (New York: Oxford University Press, 1989).
Stevens, Tim, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33/1 (2012), 148-170.
Taddeo, Mariarosaria, 'Deterrence and Norms to Foster Stability in Cyberspace', *Philosophy & Technology* 31/3 (September 2018), 323-329.
Taddeo, Mariarosaria, 'On the Risks of Relying on Analogies to Understand Cyber Conflicts', *Minds and Machines*, 26/4 (2016), 317–321.
Tannenwald, Nina, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons* (New York: Cambridge University Press, 2007).
Tor, Uri, 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40/1-2 (2017).
Trachtenberg, Marc, *History and Strategy* (Princeton: Princeton University Press, 1991).
Trager, Robert, and Dessislava Zagorcheva, 'Deterring Terrorism', *International Security* 30/3 (Winter 2005/06), 87-123.
Valeriano, Brandon, and Ryan C. Manness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015).
Wheatley, Gary F., and Richard E. Hayes, *Information Warfare and Deterrence* (Washington, DC: National Defense University Press, 1996).
Wilner, Alex, 'Contemporary Deterrence Theory and Counterterrorism: A Bridge too Far?' *NYU Journal of International Law and Politics* 47/2 (2015).
Wilner, Alex, 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies* 34/1, (2011), 3-37.
Wirtz, James J., 'How Does Nuclear Deterrence Differ from Conventional Deterrence?', *Strategic Studies Quarterly* 12/4 (Winter 2018), 58-75.
Yost, David S., 'Assurance and US Extended Deterrence in NATO', *International Affairs* 85/4 (Jul., 2009), 755-780.
Zagare, Frank C. and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge University Press, 2000).
Zagare, Frank C., 'Classical Deterrence Theory: A Critical Assessment', *International Interactions*, 21 (1996), 365–87.
Zagare, Frank C., *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987).