ISBN 978-88-255-3320-0
ISSN 1129-2113
DOI 10.4399/9788825533200-5
pp. 59-84

NOTE E COMMENTI

LO SPIONAGGIO ECONOMICO NEL DIRITTO INTERNAZIONALE

Catello Avenia*

Sommario: 1. *Premessa.* – 2. *Le (discordanti) posizioni della dottrina.* – 3. *Lo spionaggio associato ad un fatto internazionalmente illecito.* – 4. *Il concetto di intervento quando applicabile allo spionaggio (ed in particolare a quello economico).* – 5. *Lo spionaggio economico.* – 6. *Gli effetti dello spionaggio economico sui trattati internazionali.* – 7. *Responsabilità degli Stati per atti di spionaggio economico.* – 8. *segue: Le contromisure.* – 9. *Le questioni sollevabili alla luce dell'art. 10-bis della Convenzione di Parigi.* – 10. *Conclusioni.*

1. "No country poses a broader, more severe long-term threat to our nation's economy and cyber infrastructure than China. […] China's goal, simply put, is to replace the U.S. as the world's leading superpower, and they're using illegal methods to get there". Queste le dichiarazioni del Direttore dell'FBI, Chris WRAY, rilasciate nel corso di una conferenza stampa al Dipartimento di Giustizia statunitense in Washington nell'ottobre 2018[1]. Quasi anticipando un inquietante risvolto della guerra commerciale tra Stati Uniti e Cina, tutt'ora in atto: l'arresto in Canada (l'1 dicembre 2018) e su richiesta degli Stati Uniti, del CFO della Huawei, Meng WANZHOU. L'accusa formulata fu di cospirazione finalizzata alla frode alle istituzioni internazionali sulla base di una possibile violazione, da parte della Huawei, delle sanzioni statunitensi imposte all'Iran. Rilasciato su cauzione, l'alto dirigente è stato poi formalmente in criminato dai pubblici ministeri statunitensi nel gennaio 2019, per frode, ostacolo alla giustizia ed appropriazione indebita di segreti commerciali. La compagnia cinese si è difesa sostenendo che non esiste alcun legame con il governo di Pechino né che la piattaforma informatica utilizzata dalla Huawei venisse impiegata dal governo centrale per spiare clienti privati o istituzionali. Va però detto che, al momento, non esistono prove di quanto sostenuto dall'accusa né che i dati raccolti siano stati

* Professore a contratto in Diritto internazionale umanitario (Università Telematica Pegaso), già Ricercatore a t.d. IUS/13 (Università Telematica eCampus), Dottore di Ricerca in Scienza Politica e Istituzioni in Europa (Università degli Studi di Napoli Federico II), Staff Member Progetto Jean Monnet Fu.C.C.E., Avvocato.

[1] *FBI Director Christopher Wray answers questions from reporters during a news conference at the Justice Department in Washington*, U.S., October 26, 2018, in https://www.reuters.com/article/us-china-cyber-usa/u-s-allies-slam-china-for-economic-espionage-spies-indicted-idUSKCN1OJ1VN.

effettivamente utilizzati[2]. Le operazioni di spionaggio industriale da parte della Cina ai danni delle imprese statunitensi ormai non si contano più e riguarderebbero i più disparati settori industriali[3]. Ma non solo Stati Uniti. Anche Canada, Giappone, Paesi Bassi e Svezia avrebbero messo in campo strumenti per contrastare le attività di spionaggio informatico cinese.

Rob, replicate and replace, quindi. Sottrarre i segreti di un'impresa estera, replicare esattamente ciò che essa produce ed infine, sostituire la stessa sul mercato, dopo averne procurato il fallimento. Il tutto, ovviamente, in modo clandestino – a distanza od entrando sul territorio dello Stato straniero – e senza autorizzazione alcuna da parte dello Stato vittima. È il fenomeno dello spionaggio economico, una vera e propria minaccia nazionale, se non forse la principale, viste le conseguenze deleterie per l'economia. *È* fuori dubbio che lo Stato maggiormente esposto (e colpito) dal fenomeno in parola siano gli Stati Uniti d'America. Costantemente attivi nell'opera di contrasto dello spionaggio economico[4], questi hanno confermato che il fenomeno potrebbe comportare la distruzione di intere porzioni dell'economia nazionale con

---

[2] T. Lahiri, M. Hui, *How Huawei became America's tech enemy No. 1*, May 28, 2019, in https://qz.com/1627149/huaweis-journey-to-becoming-us-tech-enemy-no-1/; Z. Doffman, *Huawei accused of theft and dubious ethics. But that's not the worst of it*, May 25, 2019, in https://www.forbes.com/sites/zakdoffman/2019/05/25/huawei-accused-of-theft-and-dubious-ethics-why-it-should-come-as-no-surprise/#43259915.

[3] Un interessante studio ne conta addirittura 274 negli ultimi due decenni e sempre condotte dalla Cina ai danni degli Stati Uniti, N. Eftimiades, *Uncovering Chinese Espionage in the US. A detailed look into how, why, and where Chinese spies are active in the United States*, Nov. 28, 2018, in https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/.

[4] L'*Economic Espionage Act* del 1996, firmato dall'allora presidente Clinton nell'ottobre 1996, introduceva due nuovi reati federali comportanti il furto di segreti commerciali. L'Act ha due obiettivi: (1) prevenzione del furto di segreti commerciali specificatamente da parte di un agente governativo straniero o di altra persona che agisce per conto di un governo straniero e (2) protezione da furto di segreti commerciali da parte di chiunque. Oltre ad applicarsi ai reati commessi negli Stati Uniti, trova applicazione anche quando il fatto è commesso al di fuori del territorio se l'autore del reato (privato cittadino od un'impresa) è statunitense. S. Simon, *The Economic Espionage Act of 1996*, in *Berkeley Technology Law Journal*, vol. 13, 1998; R.C. Dreyfuss, O. Lobel, *Econoimic espionage as reality or rethoric: equating trade secrecy with national security*, in *Lewis & Clark Law Review*, vol. 2, 2016, pp. 427-434. Sebbene l'Economic Espionage Act del 1996 costituisca la principale misura statunitense di contrasto del fenomeno dello spionaggio economico, presenta numerose lacune a partire dalla sua scarsa capacità di comportarsi quale efficace deterrente. Basti considerare che il numero di furti di proprietà intellettuale è comunque in crescita e che, spesso, è difficile rinvenire responsabilità statali dietro l'atto illecito. D.P. Fidler, *Economic cyber espionage and international law: controversies involving government acquisition of trade secrets through cyber technologies*, in *American Society of International Law*, vol. 17, issue 10, mar. 2013; M. Reid, *A comparative approach to economic espionage: is any nation effectively dealing with this global threat?*, in *University of Miami Law Review*, vol. 70, 2016, pp. 46-69. Nel complesso, nonostante i suoi limiti, l'Act si è comunque rivelato un progresso sostanziale nella lotta allo spionaggio industriale, introducendo uno standard nazionale che disciplina l'appropriazione indebita di segreti commerciali, completando la moltitudine di leggi federali e statali che erano state precedentemente utilizzate con risultati decisamente inferiori.

effetti paragonabili a quelli generati da un attacco terroristico[5]. Principali indiziati di tale attività illecita sarebbero la (già citata) Cina, l'Iran e la Russia[6]. Sebbene anche gli Stati Uniti siano stati coinvolti in un recente caso di spionaggio (sebbene non di tipo economico) ai danni della Germania[7].

Da queste brevi righe è immediato comprendere come parlare di spionaggio economico significhi coinvolgere nel discorso diversi soggetti quali gli Stati, le imprese private, le organizzazioni internazionali, finanche gli individui. Si è passati dallo spionaggio di guerra (c.d. tradizionale) a quello economico, molto più pericoloso, invasivo e dannoso in quanto più sofisticato, subdolo ed imprevedibile visto che, spesso, le sue vittime ignorano l'autore dell'illecito (se esso sia un soggetto privato oppure se dietro di esso si celi uno Stato), ne possono prevedere/prevenire le conseguenze dell'atto. Ci troviamo dinanzi ad un fenomeno che merita attenzione ed approfondimento non solo per i suoi effetti e le sue conseguenze sull'economia dello Stato vittima (e per riflesso dell'economia mondiale) quanto per la sua velocità nel cambiare pelle, giungendo ad interessare (nella sua ultima versione) il furto della proprietà intellettuale.

Nel presente lavoro, previo inquadramento giuridico del fenomeno, accennate le definizioni ed evidenziate le dovute differenze tra le due tipologie di spionaggio, si rifletterà sulla posizione attuale assunta dal diritto internazionale consuetudinario nei confronti dello spionaggio economico, sulle varie convenzioni (e successive modifiche) che hanno contemplato la tematica e sulle eventuali responsabilità in capo agli Stati (non tralasciando di citare alcuni casi di spionaggio economico). Da ultime, le possibili soluzioni.

2. In origine, il concetto di spia e di spionaggio risultavano intimamente legati a quello di guerra[8] e di conseguenza la dottrina si è per lungo tempo interessata

---

[5] S. Stock, M. Bott, M. Horn, *Stolen secrets: with economic espionage on the rise, Silicon Valley must better protect secrets, Feds Warn*, in https://www.nbcbayarea.com/investigations/Stolen-Secrets-Economic-Espionage-Silicon-Valley-Federal-Warning-505814301.html, 13 feb. 2019.

[6] National Counterintelligence and Security Center, *Foreign economic espionage in cyberspace*, 2018, in https://www.dni.gov/files/ncsc/documents/news/20180724-economic-espionage-pub.pdf; L. Laskai, A. Segal, *A new old threat. Countering the return of Chinese industrial cyber espionage*, in https://www.cfr.org/report/threat-chinese-espionage, 06 dec. 2018.

[7] Nel 2014 gli Stati Uniti sono stati accusati di spionaggio contro la Germania, suo partner nato. Precisamente, si addebiterebbero agli Stati Uniti, i reati di corruzione di spie dipendenti di dipartimenti governativi tedeschi al fine di ottenere informazioni riservate; l'utilizzo dell'Ambasciata statunitense e di altri edifici situati in Germania al fine di monitorare le comunicazioni del governo e la manipolazione degli impianti di telecomunicazione all'interno del paese, nonché l'installazione di spyware sui computer ed il monitoraggio del governo tedesco e delle comunicazioni commerciali operando dal territorio degli Stati Uniti. P. Terry, *United States espionage against Germany and public international law*, in *Revue québécoise de droit international*, vol. 28, 2015.

[8] B. Warusfel, *Le cadre juridique et institutionnel des services de renseignement*, in *Le reinsegnement à la française*, Economica, 1998, p. 400 ("Historiquement, le droit international a été le premier

solo alla figura della spia utilizzata nei conflitti armati[9]. È significativo, poi, notare come una definizione del termine spionaggio non sia desumibile dai dizionari di diritto internazionale pubblico ove, per altro, si parla solo di spia ma sempre con riferimento a quella impiegata in guerra[10]. Effettivamente lo spionaggio in tempo di pace è ignorato dal diritto internazionale[11] e, fatta eccezione per il diritto internazionale umanitario, non esiste una norma che ne affermi la sua liceità o meno[12].

Su quest'ultimo punto, il dibattito in dottrina è ancora vivo. I sostenitori di una illiceità, si rivedono nelle argomentazioni del Wright, quando scrive che: "the

---

à prendre en compte juridiquement les activités des services secrets. Mais il s'est uniquement intéressé à l'espionnage dans le cadre très particulier du temps de guerre"). Posto che lo spionaggio in parola non è vietato dal diritto dei conflitti armati (ma resta punibile dalla norma penale nazionale) e che gli elementi costitutivi sono la clandestinità delle operazioni ed il carattere della confidenzialità e rilevanza militare delle informazioni raccolte (o per meglio dire, sottratte), l'Annesso alla IV Convenzione del Regolamento de l'Aja sulle leggi e gli usi della guerra terrestre (18 ottobre 1907), si limita a definire il concetto di spia. L'art. 29 del citato Annesso, infatti, definisce una spia in tempo di guerro come colui che "agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la Partie adverse. Ainsi les militaires non déguisés qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, ne sont pas considérés comme espions. De même, ne sont pas considérés comme espions: les militaires et les non militaires, accomplissant ouvertement leur mission, chargés de transmettre des dépêches destinées, soit à leur propre armée, soit à l'armée ennemie. A cette catégorie appartiennent également les individus envoyés en ballon pour transmettre les dépêches, et, en général, pour entretenir les communications entre les diverses parties d'une armée ou d'un territoire". Le spie, in tempo di guerra, al pari dei sabotatori e dei mercenari non vengono considerati combattenti e pertanto non godono di privilegio e/o tutele.

[9] "… il n'y a d'espions qu'en temps de guerre et qu'on ne saurait juridiquement donner cette qualification aux individus, qui, en temps de paix, se livrent aux mêmes pratiques". V. Colonieu, *L'espionnage au point de vue du droit international et du droit pénal français*, Librairie nouvelle de droit et de jurisprudence, Paris, 1888, p. 7. Avendo lo spionaggio quale principale accezione quella militare (compreso quando praticato in tempo di pace), "traditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate in the event of capture. And yet espionage has always played a prominent role in international relations" (R. Falk, *Foreword*, in R. Stanger, *Essays on espionnage and international law*, Ohio State University Press, 1962, p. v).

[10] Ad esempio, il manuale di Daillier e Pellet (*Droit international public*, 6e éd., Librairie générale de droit et de jurisprudence, Paris, 1999) comprende nel suo indice sei corrispondenze del termine spionaggio, mentre quelli di Combacau (*Droit international public*, 4e éd., Montchrestien, Hachette Bnf, 1999), Alland (*Droit international public*, 1re éd., Presser Universitaires de France, Paris, 2000), Carreau (*Droit international*, 6e édition, Pedone, Paris, 1999) non ne presentano alcuna.

[11] "Traditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate in the event of capture". (R.A. Falk, *Foreword*, *op. cit.*)

[12] R.R. Baxter, *So-Called 'Unprivileged Belligerency'– Spies, Guerrillas, and Saboteurs*, in *British Yearbook International Law*, vol. 28, 1951, p. 323. C.D. Baker, *Tolerance of International Espionage: A Functional Approach,* in *American University International Law Review*, vol. 19, 2004, p. 1092. "International law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation".

legitimacy of espionage in time of war arises from the absence of any general obligation of belligerents to respect the territory or government of the enemy State, and from the lack of any specific convention against it. […] In time of peace, however, espionage and, in fact, any penetration of the territory of a State by agents of another State in violation of the local law, is also a violation of the rule of international law imposing a duty upon States to respect the territorial integrity and political independence of other States"[13].

Per altra dottrina, lo spionaggio in tempo di pace sarebbe da considerarsi quale atto contrario al diritto internazionale in quanto costituirebbe una violazione della sovranità territoriale dello Stato vittima dell'illecito oltre che rappresentare un pericolo per la cooperazione pacifica tra gli Stati[14]. Una posizione piuttosto ambigua, invece, viene assunta da chi, dopo aver sostenuto che non bisogna confondere il mezzo con il fine, che "l'espionnage fait appel à des moyens qui en eux-mêmes constituent des actes contraires au droit international"[15] e che l'atto di spionaggio rientrerebbe negli atti ostili, concludono ritenendo che "d'une manière plus générale, il est possible de concevoir que l'espionnage soit un acte contraire au droit international, dans la mesure où il se confond avec la violation de l'obligation de respecter la souveraineté des autres Ètats"[16].

Altri ancora[17], si rifanno agli arresti della Corte Permanente di Giustizia Internazionale nel noto caso *Lotus* del 1927 "selon laquelle les limitations à l'indépendance des Ètats ne se présument pas: en l'absence de règles prohibitives venant limiter sa liberté, chaque Ètat reste libre d'adopter les principes qu'il juge les meilleurs et les plus convenables"[18]. Diversamente detto, l'attività di spionaggio al pari di "toute activité qui n'est pas interdite expressément est jugée légitime et donc per-

---

[13] Q. Wright, *Espionage and the doctrine of non-intervention in internal affaire*, in R. Stanger, Essays on espionage and international law, *op. cit.*, p. 12

[14] "Espionage in peacetime is contrary to international law, even if it does not involve any trespass". I. Delupis, *Foreign warships and immunity for espionage*, in *American Journal of International Law*, 1984, volume 78, n. 1, p. 67.

[15] G. Cohen-Jonathan, R. Kovar, "L'espionnage en temps de paix", in *Annuaire française de droit international*, 1960, p. 246. Ma non bisogna confondere il mezzo (illecito, secondo il diritto internazionale) con lo scopo (illecito, secondo le norme interne ma lecito per il diritto internazionale). Infatti sempre più spesso i governi, quando interessati da un atto di spionaggio comportante anche una violazione della propria sovranità territoriale, pongono sullo stesso piano i due aspetti della vicenda, ossia la violazione dell'integrità territoriale e l'atto di spionaggio.

[16] Id., p. 254.

[17] J. Stone, *Legal problems of espionage in conditions of modern conflict*, in R. Stanger, Essays on espionage and international law, *op. ci*t., pp. 33-34 ; M. Dauses, D. Wolf, *L'espionnage par satellites et l'ordre international*, in *Revue générale de l'air et de l'espace*, n.1, 1973, p. 295 ; E.Rauch, "Espionage" in Encyclopedia of public international law, North-Holland, 1995, volume 2, p. 116.

[18] W. Prosper, *Le droit international public en quête de son identité. Cours général de droit international public*, in *Collected Courses of the Hague Academy of International Law*, The Hague Academy of International Law, tome 237 (1992-vi), Martinus Nijhoff Publishers, 1996, p. 210.

mise en droit international public"[19] e lo spionaggio non sarebbe vietato dal diritto internazionale, indipendentemente dal fatto che sia effettuato tramite agenti inviati in un territorio straniero dallo spazio aereo od extra-atmosferico o grazie ai sistemi informatici, da un territorio limitrofo o dall'alto mare[20]. Accettando il carattere lecito degli atti di spionaggio, pur sottolineandone la loro capacità di nuocere alle relazioni tra gli Stati, parte della dottrina ha preferito far rientrare gli atti in parola nella categoria degli atti non amichevoli tra Stati[21].

Partendo dall'affermazione dell'Acheson in base alla quale lo spionaggio costituisce "the underworld of international relations"[22], la questione invece muta natura e ci si può chiedere quando la responsabilità internazionale di uno Stato possa essere invocata in presenza di un atto di spionaggio, stante la sua liceità. Da questa prospettiva, solo un atto associato ad un fatto internazionalmente illecito sarebbe suscettibile di far sorgere in capo ad uno Stato dei profili di responsabilità, residuando in alternativa una responsabilità individuale.

Parte della dottrina[23], pur ammettendo la legittimità dello spionaggio, considera la pratica in parola come un atto ostile[24] tra Stati, "c'est-à-dire à cette catégorie d'actes d'un Ètat dont se plaint un autre Ètat sans pretender qu'ils soient contraires au droit des gens, mais en alléguant qu'ils sont de nature à rendre plus difficiles les

---

[19] M. Dauses, D. Wolf, *op. cit.*, p. 295.

[20] T. Stein, T. Makauhn, *Volkerrechtliche Aspekte von Informationsoperationen*, in *Zeitschrift für ausländisches* öffentliches *recht und völkerrecht*, 2000, volume 60/1, pp. 32-33. "Spionage und Aufklarung als solche sind nicht verboten, unabhangig davon, ob sie durch Agenten auf dem fremden Territorium, aus dem Luftoder Weltraum oder elektronisch vom benachbarten Territorium. oder von der Hohen See aus erfolgen".

[21] G. Demarest, *Espionage in international law*, in *Denver Journal of International Law & Policy*, vol. 24, 1996, p. 347.

[22] J.M. Sweeney, C.T. Oliver, N.E. Leech, *Powers case et beyond trespass: espionage as a state offense*, in *Cases and materials on the international system*, 1988, 3e édition, p. 281.

[23] In particolare G. Cohen-Jonathan, R. Kovar, *op. cit.*, p. 252; G. Demarest, *op. cit.*, p. 347.

[24] Va subito notato che parte della dottrina classifica l'atto ostile come atto politico o diplomatico piuttosto che giuridico (H. Weber, *Unfriendly act*, in *Encyclopedia of public international law*, North-Holland, 1982, vol. 4, pp. 252-253; C. Parry, J.P. Grant, *Unfriendly act*, in *Encyclopedic dictionnary of international law*, Oceana Publications Inc., New York, 1986, p. 411); di conseguenza, la prassi mostra che gli Stati preferiscono una soluzione politica ai casi di spionaggio, sempre che il diritto internazionale non preveda un meccanismo a sé stante. Diversi fattori contribuiscono alla necessaria predominanza di questo approccio politico. In primo luogo, un atto di spionaggio commesso da un individuo è solo eccezionalmente attribuibile, in pratica, allo Stato beneficiario (P. Daillier, A. Pellet, *op. cit.*, p. 753) e può solo comportare un deterioramento delle relazioni tra i governi interessati. In secondo luogo, anche in presenza di un controllo dello Stato istigatore sulla spia, lo Stato vittima si dimostrerà più interessato al risarcimento del danno che ha subito rispetto al beneficio che un altro Stato ha potrebbe trarre in ragione del carattere reciproco delle attività di spionaggio fondate sul principio del "tu quoque". In base a questo principio, uno Stato non sarebbe concesso lamentarsi del comportamento di un altro Stato, quando si comporta allo stesso modo nelle stesse occasioni. (W.-W. Langkau, *Vôlker – und landesrechtliche Problème der Kriegs – und Friedensspionage*, Wûrzburg, 1970, p. 165; M. Dauses, D. Wolf, *op. cit.*, p. 295).

relations entre les deux gouvernements"[25]. Diversamente detto, "while clandestine information gathering will continue to be considered an unfriendly act between nations, such activity does not violate international law"[26].

La classificazione dello spionaggio quale atto ostile presuppone che sia materialmente possibile imputarlo ad un dato Stato. Ma, fatta eccezione per i casi in cui il coinvolgimento di un governo in un atto di spionaggio sia manifesto (sia perché lo riconosce ufficialmente, sia perché gli agenti catturati sono personale accreditato presso lo Stato vittima oppure ancora perché l'atto di spionaggio è corredato dalla commissione di atti illeciti internazionalmente rilevanti), la partecipazione diretta o indiretta di uno Stato alle attività di ricerca delle informazioni a danno di altri governi è solitamente difficile da individuare. La questione si pone prima di tutto in merito agli agenti dei servizi segreti inviati in territorio straniero in missione. In effetti, è stato sostenuto[27] che in conformità del principio dell'immunità dalla giurisdizione degli atti dello Stato e dei suoi organi, il ragionamento seguente potrebbe essere applicato a tutti i casi di spionaggio commesso da funzionari pubblici: lo Stato ed i suoi organi godono di tale immunità purché non vi sia una violazione di una norma internazionale. Questo ragionamento viene contestato da Bothe[28] che ricorda come la regola dell'immunità giurisdizionale degli organi statali non sia illimitata ed a fondamento della sua tesi, l'autore cita casi di spionaggio in cui, mancando l'immunità diplomatica per gli agenti stranieri, i tribunali competenti hanno condannato questi ultimi. Nel frequente caso in cui uno Stato ottenga informazioni trasmesse da un individuo che è cittadino dello Stato vittima, la sua responsabilità può essere difficilmente ravvisata visto che nè il coinvolgimento dei propri agenti né la violazione della sovranità territoriale dello Stato spiato possono essere invocate da quest'ultimo[29].

---

[25] G. Cohen-Jonathan, R. Kovar, *op. cit.*, p. 252.

[26] G. Demarest, *Espionage in international law*, in *Denver Journal of International Law & Policy*, 1996, volume 24, p. 437.

[27] P. Daillier, A. Pellet, *op. cit*., 447-448 (§ 290).

[28] M. Bothe, *Die strafrechtliche Immunitàt der Staatsorgane*, in *Zeitschrift für ausländisches* öffentliches *recht und Völkerrecht*, n. 31, 1971, p. 252.

[29] In effetti, "la responsabilité internationale des Ètats à raison de l'activité de leurs services secrets à l'étranger ne donne pas lieu habituellement à des développements juridiques très abondants. Par leur nature même, les affaires de ce type appellent un règlement discret sinon occulte, par voie de négociations directes se soldant par une indemnisation forfaitaire de l'ensemble des dommages". G. Apollis, *Le règlement de l'affaire du Rainbow Warrior*, in *Revue Générale de Droit International Publique*, vol. 1, 1987, p. 10. Inoltre, mentre le azioni degli agenti sono indiscutibilmente attribuibili allo Stato, ciò non toglie "la plupart du temps, les moyens de prouver l'existence de ce lien [entre les agents et l'Ètat d'envoi] font défaut; il est, dans la plupart des cas, extrêmement difficile d'apporter la prevue que l'action de ces individus relève, en dernière analyse, de celle d'un fonctionnaire étatique, qui les dirige et les contrôle". J.-P. Queneudec, *Les fonctionnaires de fait et les agents secrets*, in *La responsabilité internationale de l'*Ètat pour les fautes personnelles de ses agents, in *Librairie générale de droit et de jurisprudence*, 1966, p. 47. In definitiva, "les gouvernements utilisent les services d'honorables correspondants, d'espions et autres agents moins qu'officieux dont ils se gardent, et pour cause, de couvrir les exploits, de manière à ne pas s'en voir imputer la responsabilité". A. Co-

Va altresì ricordato che, secondo il diritto internazionale, la spia non gode di una posizione particolare in quanto non è considerata agente ufficiale dello Stato (presuntivamente) mandante. Questo significa che si può configurare una responsabilità individuale e che la sua azione non può essere giustificata quale esecuzione di un ordine impartitogli dal suo Stato di origine. Da quanto testè accennato, si comprende che la responsabilità di uno Stato viene in evidenza solo quando la spia agisce per conto dello Stato ossia in qualità di organo di questo; diversamente, è da escludere la responsabilità statale[30]. Si tratta, comunque, di atti che rischiano di indebolire il principio delle "relations amicales" tra gli Stati come stabilito nella Carta delle Nazioni Unite all'art. 1.2.

3. Occorre distinguere tra atti di spionaggio che comportano la violazione della sovranità territoriale di un altro Stato ed atti che non presentano tale illecito[31]. Il primo tipo di spionaggio riguarda il caso in cui l'agente-spia è presente in territorio straniero per raccogliere (clandestinamente) informazioni ed in questo caso è configurabile una responsabilità in capo al suo Stato di origine. Nel secondo caso, si fa ricorso a mezzi tecnologici e si sfrutta lo spazio internazionale od il territorio del proprio Stato per far partire l'azione. Anche in questo caso la raccolta di dati è comunque clandestina perché manca il consenso dello Stato interessato (sebbene, per quanto riguarda gli spazi internazionali, come l'alto mare e lo spazio esterno, vi sia libertà d'uso).

L'invio da parte di uno Stato di una spia su un territorio di un altro Stato[32], quale che sia il modo di attraversamento dei confini (per terra, aria o mare), costituisce una palese violazione della sovranità territoriale dello Stato vittima e comporta una responsabilità in capo allo Stato mandante. Bisogna però distinguere se la violazione commessa consiste nell'attraversare lo spazio aereo oppure le acque territoriali. È ben noto che lo *status* giuridico dello spazio extra-atmosferico, riposando sulla libertà di suo utilizzo da parte di tutti gli Stati[33], non lascia spazio a rivendicazioni di sovranità. Ma è pur vero che non esiste un criterio di delimitazione fisica tra spazio aereo e spazio extra-atmosferico e, tra l'altro, la sovranità di uno Stato, relativamente allo spazio atmosferico, è fissata nella sua dimensione verticale[34].

CATRE-ZILGIEN, *L'affaire Argoud. Considérations sur les arrestations internationalement irrégulières*, Èditions A Pedone, Paris, 1965.

[30] H. WEBER, *Grundkurs Völkerrecht, Das internationale Recht des Friedens und der Friedenssicherung*, Frankfurt am Main, Metzner, 1977, pp. 122 ss.; P. DAILLIER, A. PELLET, *Droit international public*, *op. cit.*, pp. 557 ss.

[31] Sul punto, A. DEEKS, *An international legal framework for surveillance*, in *Virginia Journal of International Law*, vol. 55, 2015.

[32] E così dicendo, ci riferiamo alla prima tipologia di atti di spionaggio ossia quella che comporta la violazione della sovranità territoriale di un altro Stato.

[33] P. DAILLIER, A. PELLET, *Droit international public*, *op. cit.*, pp. 1208-1210.

[34] Secondo Kish, "the upper flight height of aircraft and the lower orbit of spacecraft determine the zone for the boundary between airspace and outer space" (J. KISH, *International law and espionage*, Martinus Ni-

Nonostante i progressi tecnici compiuti nella raccolta remota di informazioni, non sono pochi i casi di sconfinamento, in acque territoriali, di imbarcazioni per la raccolta di cui sopra. Mentre il sorvolo dello spazio aereo di uno Stato è sottoposto all'autorizzazione di quest'ultimo[35], nel diritto del mare è riconosciuto il diritto alle navi da guerra ad un passaggio inoffensivo nel mare territoriale di uno Stato terzo[36]. In virtù dell'art. 19.2 della Convenzione di Montego Bay del 1982, un tale passaggio non è considerato inoffensivo se il "navire se livre […] à la collecte de renseignements au détriment de la défense ou de la sécurité de l'Ètat côtier"[37]. Quanto ai sottomarini, l'articolo 20 precisa che essi sono "tenus de naviguer en surface et d'arborer leur pavillon" quando nel mare territoriale. La priorità della sicurezza costiera (sugli interessi dello Stato beneficiante del diritto del diritto del passaggio inoffensive) alla fine nega l'ammissibilità dello spionaggio nel mare territoriale[38].

---

jhoff Publishers, La Haye, 1995, p. VIII) e questo, all'occorrenza, comporterà un problema di natura giuridica riguardante l'intrusione di un aeromobile-spione (G. COHEN-JONATHAN, R. KOVAR, *L'espionnage en temps de paix*, in *Annuaire Français Droit International*, 1960, pp. 247-248). Il diritto internazionale riconosce a ciascun Stato il diritto di intercettare e di impedire ad un aeromobile il sorvolo del suo spazio aereo, senza consenso (P. DAILLIER, A. PELLET, *op. cit.*, p. 1198). Sin dal 1902, l'Istitut de Droit International notava nell'art. 7 della sua risoluzione sul diritto aereo che "every State has rights over its airspace which are necessary for its protection and for the suppression of espionage" (INSTITUTE OF INTERNATIONAL LAW, *Resolution on the Law of the Air*, in Yearbook of the Institute of International Law, Bruxelles, 1902, p. 32). In sintonia, l'art. 9.a della Convenzione di Chicago sull'aviazione civile internazionale ove si precisa che gli Stati contraenti possono interdire il sorvolo di alcune parti del proprio territorio "pour des raisons de nécessité militaire ou de sécurité publique". Pertanto, "les opérations d'interception doivent être menées selon certaines règles posées tant par le droit international général que par le droit aérien" (G. GUILLAUME, *Le vol KE 007*, in *Les grandes crises internationales et le droit*, Le Seuil, Paris, 1994), specificamente agli aeromobili civili.

[35] P. DAILLIER, A. PELLET, *op. cit*., p. 1202.

[36] Art. 17 Convenzione di Montego Bay del 1982: "[…] les navires de tous les Ètats, côtiers ou sans littoral, jouissent du droit de passage inoffensif dans la mer territoriale".

[37] Art. 19, Signification de l'expression passage inoffensive, Convention des Nations Unies sur le droit de la mer, 1982.

[38] J. KISH, *op. cit.*, p. 96. Per quanto riguarda una nave da guerra che non rispetta queste regole, che può essere integrata da leggi e regolamenti nazionali in questo settore, lo Stato costiero ha un potere limitato; infatti, ai sensi dell'articolo 30 della convenzione di Montego Bay, quest'ultimo deve accontentarsi di "exiger que ce navire quitte immédiatement la mer territoriale". D'altro canto, "l'Ètat du pavillon porte la responsabilité internationale […] de tout dommage causé à l'Ètat côtier du fait de l'inobservation par un navire de guerre […] des lois et règlements de l'Ètat côtier relatifs au passage dans la mer territoriale ou des dispositions de la Convention ou d'autres règles du droit international" (art. 38, Convenzione di Montego Bay). Nel caso in cui una nave da guerra, sospettata di aver condotto attività di spionaggio in acque territoriali, rientrerebbe nella legislazione dello Stato costiero leso e sorgerebbe la questione dell'immunità del naviglio e del suo equipaggio. In realtà "[…] a well established rule of international law that warships are immune from legal process […] of foreign authorities. This immunity applies to the commander and the crew, as well as to the ship itself" (I. DELUPIS, Foreign warships and immunity for espionage, in *American Journal of International Law*, 1984, vol. 78, n° 1, p. 55). Inoltre, la commissione di atti ufficiali, illeciti ai sensi del diritto internazionale, non comporta la perdita di tale immunità. Non essendo lo spionaggio vietato dal diritto internazionale, lo Stato costiero vittima di una violazione delle sue acque territoriali commessa al fine di ottenere informazioni, non

4. Ma l'atto di spionaggio (*lato sensu*) può essere considerato quale ingerenza negli affari interni di uno Stato? Secondo il diritto internazionale "intervention is prohibited when it interferes in matters in which each state is permitted to decide freely by virtue of the principle of state sovereignty"[39].

Il termine *intervento* è comunemente usato per connotare ogni atto di interferenza (anche economica) da parte di uno Stato negli affari di un altro; la prassi statale, invece, nel tollerare ed incoraggiare l'attività economica transfrontaliera dimostra che non si potrebbe sostenere che il diritto internazionale proibisca ogni forma di coinvolgimento esterno negli affari economici interni di uno Stato, al pari dell'impegno diplomatico che non viene considerato un'ingerenza e quindi non un atto illecito[40]. La tradizionale formulazione di intervento come "dictatoral interference" con conseguente subordinazione della volontà di uno Stato sovrano ad un altro, non è però sufficiente per comprendere i contorni delle interferenze proibite[41]. Come conseguenza della sovranità e del controllo statale del territorio, la norma del non intervento proibisce agli Stati di imporre coercitivamente la propria volontà alle questioni interne ed esterne di altri Stati, cyberspazio compreso [42]. Per parte della dot-

può lamentarsi dell'atto di spionaggio quanto piuttosto della violazione delle norme del diritto del mare ossia di eventuale mancato rispetto del passaggio inoffensivo (A. Manin, *L'*échouement *du Whiskey 137 et le droit de la mer*, in *Annuaire Française de Droit International*, 1982, p. 699). Inoltre, quando si verificano tali incidenti, lo Stato costiero si trova spesso di fronte ai problemi posti dalla posizione della nave e dalla natura delle sue attività al momento dell'evento.

[39] C.C. Joyner, C. Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, in *European Journal of International Law*, vol. 12, 2001, p. 847.

[40] Q. Wright, *Legality of Intervention under the UN Charter*, in *American Journal of International Law Procedure*, vol. 51, 1957, pp. 79, 88.

[41] L. Oppenheim, *International Law: a treatise*, Roxburgh, 1920, § 134; v. anche E.C. Stowell, *Intervention in International Law*, Byrne, Washington d.c., 1921, p. 317.

[42] Report of the International Law Commission, 53d Sess., Apr. 23-June 1, July 2-Aug. 10, 2001, u.n. Doc. a/56/10 at 180; gaor, 56th Sess., Supp. No. 10 (Aug. 10, 2001) ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State…"). Ovviamente, la valutazione della liceità o meno degli interventi nel cyberspazio dipenderà da molti fattori circostanziali che dovranno essere valutati caso per caso. Per comprendere quali saranno gli atti previsti come illecito dal principio del non intervento, bisognerà considerare il principio di sovranità e sua eventuale violazione. Gli atti dovranno essere coercitivi e mirare a quelle azioni nelle quali lo Stato ha il diritto di libera scelta. Nel valutare i vari modi in cui la sovranità di uno Stato può essere violata, compreso il cyberspazio, sarebbe utile descrivere i diversi atti, dall'intervento armato alla mera minaccia dell'uso della forza (per quanto riguarda gli interventi c.d. materiali), dalla manipolazione dei risultati elettorali di uno Stato terzo tramite internet per impedire a questo di decidere liberamente il proprio sistema politico ad atti (o meglio, interventi) di spionaggio economico volti a destabilizzare l'economia dello Stato concorrente. G.D. Brown, O.W. Tullos, *On the Spectrum of Cyberspace Operations*, in *Small Wars Journal*, 2012, in www.smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations; R. Higgins, *Intervention and International Law*, in *Intervention in World Politics*, Hedley Bull, 1984, pp. 29-30; M.S. McDougal, F.P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, in *Yale Law Journal*, vol. 67, 1985, pp. 771, 779.

trina, le operazioni informatiche eseguite clandestinamente in uno Stato violano il principio di non intervento e di conseguenza si possono qualificare come atti internazionalmente illeciti, specialmente quando volti a coartare (e non solo influenzare) il governo dello Stato bersaglio in questioni riservate[43]. Proprio come l'atto (materiale) internazionalmente illecito commesso da uno Stato che può costituire una violazione della Carta delle Nazioni Unite, del diritto internazionale umanitario, degli altri obblighi previsti da trattati, principi e convenzioni internazionali (come ad esempio l'UNCLOS o il WTO) od i fondamentali del diritto internazionale consuetudinario, così le azioni di uno Stato nel cyberspazio potrebbero rappresentare delle violazioni di varie fonti del diritto internazionale. E proprio come gli interventi di uno Stato che non raggiungono il livello di uso della forza, possono essere considerati come illeciti internazionali anche gli interventi di uno Stato che procurano danni ad un altro Stato, effettuati tramite il cyberspazio[44]. Proprio la dimensione immateriale delle nuove sfide da affrontare per l'*intelligence* e la necessità di rimanere nel campo delle misure non implicanti l'uso della forza, nonché il livello transnazionale della sottrazione di segreti industriali (o se si preferisce, economici in senso più ampio) e le conseguenze sull'economia dello Stato vittima, spinsero, nel 2013, un gruppo di esperti internazionali a redigere e pubblicare il *Tallin Manual on the International Law Applicable to Cyber Warfare*, uno studio – non vincolante – su come il diritto internazionale intervenga in tale particolare dimensione conflittuale[45]. La conclusione dei lavori fu concorde nel ritenere che gli Stati, ormai, avvertono come concreto e possibile (nonché necessario) l'intervento del diritto internazionale nel cyberspazio[46].

---

[43] M.N. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, *op. cit.*, ("Cyber operations into another State violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as distinct from merely influence) the targeted State's government in matters reserved to that State.").

[44] ID., p. 44. ("In particular, a cyber operation may constitute a violation of the prohibition on intervention").

[45] M.N. SCHMITT, *Tallin Manual on the International Law Applicable to Cyber Warfare*, vol. 4, 2013, pp. 9-11. v. anche M.N.SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal Transnational Law*, vol. 37, 1999, p. 885, 886; E.T. JENSEN, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, in *Stanford Journal of International Law*, vol. 38, 2002, pp. 207, 208-209; M.N. SCHMITT, *The Law of Cyber Warfare: Quo Vadis?*, in *Stanford Law & Policy Review*, vol. 25, 2014, pp. 269-270.

[46] U.N. SECRETARY-GENERAL, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98, June 24, 2013, pp. 7-8. "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory….States must meet their international obligations regarding internationally wrongful acts attributable to them". Come riportato nel Manuale, "cyber operations into another State violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as opposed to merely influence) the targeted state's government in matters reserved to that State".

5. L'epoca nella quale viviamo è decisamente quella dell'informazione e l'importanza di raccogliere ed utilizzare le informazioni nel minor tempo possibile rispetto a quanto fatto dal "concorrente" (sia esso un privato od uno Stato) è diventato fondamentale[47]. Con l'avvento di internet, poi, la competizione economica ha trovato un nuovo spazio dove svolgersi, caratterizzata da una dimensione immateriale che rende difficile il controllo ed il contrasto da parte degli Stati coinvolti dal fenomeno[48]. La strategia utilizzata è quella di agire senza tregua, senza soluzione di continuità per demoralizzare l'avversario che, al termine di un'azione di logoramento ed un conseguente esaurimento psicologico, crolla e decide di delocalizzare, chiudere, licenziare, fallire[49].

Diversamente dallo spionaggio per scopi politici e militari, lo spionaggio economico ha come obiettivo quello di raccogliere informazioni private di proprietà di un soggetto (sia esso individuo o collegiale, pubblico o privato) al fine di fornire vantaggi allo Stato committente, evitando dispendiosi investimenti economici in ricerca e sviluppo. Le informazioni sottratte dal personale dell'*intelligence* o delle forze armate possono includere proiezioni di vendita, dati sui prezzi, elenchi di clienti, dati sullo sviluppo del prodotto, ricerca di base, strategie di marketing, piani di sviluppo, dati dei dipendenti, proposte di contratto, profitti futuri stimati, proprietà di software e pianificazione strategica[50]. È intuitivo poter distinguere lo spionaggio tradizionale da quello economico considerato lo scopo, i metodi ed il teatro degli scontri ossia la competizione economica. E se nello spionaggio tradizionale è possibile parlare di un "gioco a somma zero" cioè la reciproca accettazione dell'attività ed i benefici che ricadono su entrambi gli Stati coinvolti, nello spionaggio economico l'unico risultato possibile è quello favorevole allo Stato[51].

---

[47] D. Danet, *L'intelligence* économique: *de l'Etat à l'entreprise*, in *Les Cahiers du numérique*, vol. 3, Paris, 2002, pp. 139-170.

[48] J. Stanton, *Industrial Espionage Becoming "Big Business",* in *National Defence*, July, 2001, www.nationaldefensemagazine.org/archive/2001/July/Pages/Industrial_ Espionage7002.aspx?PF=1.

[49] E. Halby, *Intelligenza economica & tecniche sovversive. Le armi della nuova economia*, Milano, FrancoAngeli, 2003, p. 108.

[50] E. Fraumann, *Economic Espionage: Security Missions Redefined*, in *Public Administration Review*, vol. 57, 1997, p. 303.

[51] Importante distinzione tra spionaggio tradizionale e quello economico è che nel primo caso le "regole del gioco" sono ben note alle parti e questo garantisce stabilità tra gli Stati interessati dal fenomeno (e non solo nei loro confronti) (C.D. Baker, *Tolerance of International Espionage: A Functional Approach*, in *American University International Law Review*, vol. 19, 2004, pp. 1091, 1097 (si descrive lo spionaggio economico come "a functional tool that enables international cooperation"; K.W. Abbott, *"Trust But Verify": The Production of Information in Arms Control Treaties and Other International Agreements*, in *Cornell International Law Journal*, vol. 26, 1993, p. 26 ("States seeking to convey assurances may find some foreign monitoring desirable as a way to channel information"); nel secondo, invece, si genera paralisi delle economie e si destabilizza l'ordine economico globale ad un ritmo molto rapido, mettendo potenzialmente a rischio la pace e la sicurezza dell'intera comunità internazionale, complice il sistema attraverso il quale l'attività di raccolta di dati viene effettuata.

Altro elemento distintivo è la motivazione dell'attore[52], potendo distinguere tra la raccolta di informazioni che agevola i responsabili delle politiche ad anticipare le tendenze e le minacce future contro lo spionaggio economico utilizzato allo scopo di indebolire le norme di sicurezza o le politiche economiche di uno Stato. Alcuna dottrina sostiene che lo spionaggio economico e quello tradizionale coesistano nello stesso spazio del diritto internazionale, in assenza di leggi regolanti queste attività, tollerate da molti Stati[53]. Ma, diversamente dallo spionaggio tradizionale, quello economico non ha "custom of reciprocity or cooperation that states should be concerned about preserving"[54]. La domanda da porsi è se sia possibile rinvenire una distinzione giuridicamente rilevante, nel diritto internazionale, tra lo spionaggio tradizionale e quello economico. A livello nazionale, molti Stati hanno qualificato come reato lo spionaggio economico e contestano quegli Stati che lo praticano, precisando però che non esistono evidenze sulla promulgazione di leggi nazionali che autorizzino autorità governative a sottrarre segreti commerciali alle imprese di un altro Stato. La prassi statale messa in atto per contrastare lo spionaggio economico è ben diversa quando rivolta allo spionaggio tradizionale. E se la questione della liceità degli atti di spionaggio tradizionale investiva l'individuo e lo Stato mandante, con lo spionaggio economico in discussione emergono le sanzioni ed il conseguente richiesto intervento al WTO.

Le conseguenze di questa vera e propria guerra economica[55], molto più competitiva e subdola rispetto a quella "tradizionale", sono devastanti: dalla destabilizzazione del mercato al fallimento delle imprese alla disoccupazione di massa fino alla delocalizzazione forzata di imprese nazionali. Tra le tecniche utilizzate in questa nuova guerra, possiamo ricordare il *benchmarking* ovvero l'osservare ed analizzare il comportamento di un'altra società – ritenuta migliore – al fine di emularla, apprendere e quindi rendersi del tutto simile ad essa[56]. I costi della ricerca e dello sviluppo

---

[52] RA. Falk, *op. cit*., p. 58.

[53] D.P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, in *American Society International Law*, vol. 47, 2013, p. 2.

[54] C.P. Skinner, *An International Law Response to Economic Cyber Espionage*, in *Connecticut Law Review*, vol. 46, 2014, p. 1183.

[55] La definizione di guerra economica mondiale dovrebbe essere ricondotta a Bernard Esambert ed al suo *La guerre économique mondiale* (éd. Olivier Orban, 1991) per il quale "la conquête des marchés et des technologies a pris la place des anciennes conquêtes territoriales et coloniales", p. 10.

[56] In realtà, va precisato, la tecnica in parola non è illegale purché fatta con il consenso del concorrente e non in suo danno. Diversamente detto, mirare al patrimonio tecnologico di un'impresa significa compromettere la performance o l'esistenza stessa dell'impresa target. In questo caso, da semplice studio di un successo, il *benchmarking* si trasforma in vero rischio di deviazione di sapere. Prendiamo come esempio le operazioni di *reverse engineering*, ossia analisi approfondite dei prodotti, loro funzionamento, progettazione e sviluppo messi in campo dai concorrenti. R. Camp, *Benchmarking. Come analizzare le prassi delle aziende migliori per diventare i primi*, Milano, Itaca, 1991; U. Bocchino *Il benchmarking, uno strumento innovativo per la pianificazione ed il controllo strategico*, Milano, Giuffré editore, 1994.

sono decisamente elevati ed è considerato più redditizio (ma ovviamente illegale) per un concorrente tentare di distrarre i risultati ottenuti da altri per confrontarli con i propri, informarsi sui progressi fatti dai concorrenti o molto più semplicemente sottrarli. I vantaggi derivanti dal furto di tecnologia sono così elevati che alcuni governi si sono schierati in prima linea nelle operazioni di difesa in questa sfera[57].

6. Va subito chiarito che, al momento, non esiste un trattato internazionale che disciplini in modo specifico lo spionaggio economico; mentre diverse sono le convenzioni e gli accordi che vietano le azioni ritenute dannose per il commercio internazionale o lo sviluppo economico. La Convenzione di Parigi del 1883

[57] Ad esempio, il consiglio statale del contro-spionaggio statunitense nel 1996 evidenziò un piano di azione del governo sud coreano per trasferire (in modo indiretto e comunque senza autorizzazione alcuna) tecnologie. Tre anni dopo, sempre gli Stati Uniti, attraverso la propria agenzia CIA, diedero vita ad un fondo d'investimento per le nuove tecnologie consentendo all'agenzia ed ai servizi segreti americani di garantirsi un certo vantaggio economico sui concorrenti economici. Nel 2000 vide la luce il National Counter-intelligenge Executive con la missione di sostenere le infrastrutture di contro-spionaggio statunitense e di sensibilizzare le imprese nei confronti dei nuovi pericoli derivanti dallo spionaggio economico, pubblicando con regolarità dei reports sullo stato di tali pericoli e descrivendo le tecniche usate per sottrarre informazioni ad un'impresa. Il diritto internazionale proibisce alcuni tipi di coercizione economica, ad esempio quando sono utilizzati per motivi politici, incluse le sanzioni od i blocchi economici che, paralizzando l'economia di un paese, ne mina la sua libertà politica e ne impedisce di fatto la partecipazione ai mercati globali. R.B. LILLICH, *Economic Coercion and the New International Economic Order: A Second Look at Some First Impressions*, in *Virginia Journal of International Law*, vol. 16, 1976, pp. 233, 234; D. BOWETT, *Economic Coercion and Reprisals by States*, in *Virginia Journal of International Law*, vol. 13, 1972, pp. 1, 5 ("In other words, measures not illegal per se may become illegal only upon proof of an improper motive or purpose."); D. BOWETT, *International Law and Economic Coercion*, in *Virginia Journal of International Law*, vol. 16, 1975-1976, p. 249 ("It does not suggest that it is lawful to cause injury to another State by economic coercion when the motive is to further or protect the State's *political* interests."). Non possiamo trascurare l'importante precedente costituito dal giudizio reso dalla Corte Internazionale di Giustizia nello storico caso *Nicaragua v. United States*, ove fu dichiarato che questi ultimi avevano violato gli obblighi previsti dal diritto internazionale di non usare la forza contro un altro Stato e di non violarne la sovranità, sebbene l'oggetto di tale intrusione fosse l'acquisizione di informazioni segrete. (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27). Fu utilizzato uno specifico standard di interferenza nel rendere la sua decisione su quali tipi di azioni raggiungerebbero il livello di intervento vietato, rilevando che l'obiettivo specifico della coercizione deve essere quello di impedire, allo Stato vittima, di decidere liberamente; pertanto non tutti i tipi di interferenze sarebbero vietati. Nella sua decisione la Corte, inoltre, precisò e chiarì che, sebbene il mancato impiego di armi nello spionaggio economico per compiere gli atti coercitivi in parola lo qualifichi come lecito, in realtà la forma di intervento illecito non va limitata al solo uso di armi ma può assumere forme diverse in quanto quello che rende illecito l'intervento è un atto coercitivo "bearing on matters in which each state is permitted, by the principle of state sovereignty, to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy". Nel segnalato caso, è stato precisato che una cosa è scegliere di prendere le distanze economicamente da un regime non gradito; altro è infliggergli un danno economico ricorrendo a (illeciti) blocchi economici od il furto di sua proprietà intellettuale. Anche questa forma di intervento è coercitivo, intervenendo sull'indipendenza degli Stati giungendo a produrre un generale deterioramento del commercio mondiale e della stabilità finanziaria se non anche costituire una minaccia per la pace mondiale.

fu il primo accordo internazionale volto a proteggere la proprietà intellettuale, richiedendo alle nazioni firmatarie di estendere ai cittadini stranieri le tutele della proprietà intellettuale fornite ai propri cittadini, stabilendo regole uniformi sui diritti derivanti da detta proprietà[58]. Sebbene la Convenzione di Parigi non riguardi espressamente lo spionaggio economico[59], l'art. 10 sulla concorrenza sleale proibisce "any act of competition contrary to honest practices in industrial or commercial matters"[60]. Nel 1967, fu istituita la World Intellectual Property Organization ("WIPO") al fine di dar vita ad una convenzione per regolare i vari accordi sulla proprietà intellettuale (compresa la Convenzione di Parigi) e per proteggere la proprietà intellettuale in tutto il mondo[61]. La WIPO fornisce una definizione molto ampia di proprietà intellettuale al fine di includere i diritti relativi a qualsiasi invenzione o proprietà industriale o disegni, fornendo protezione contro la concorrenza sleale e "all other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields"[62].

Altro accordo in materia è il Trade-Related Aspects of Intellectual Property Rights Agreement ("TRIPS"), raggiunto nel corso dell'Uruguay Round del GATT nel 1994, che impone agli Stati membri di tutelarsi contro l'acquisizione, la divulgazione o l'uso dei segreti commerciali di uno Stato "in a manner contrary to honest commercial practices"[63]. "Honest commercial practices" sono specificate nella nota 10 e definite come 'breach of confidence,' ma la definizione non comprende l'acquisizione illecita della proprietà intellettuale. Sebbene il TRIPS si riferisca specificamente alle "confidential information" piuttosto che ai segreti commerciali, definisce tali informazioni come aventi valore commerciale ed all'art. 39 è prevista la loro protezione, in un quadro di "unfair competition". Centrale, per l'applicazione dell'art. 39.3 del TRIPS[64], è determinare quale sia la natura e la portata dell'obbligo di

---

[58] Paris Convention for the Protection of Industrial Property, art. 1, Mar. 20, 1883, 21 U.S.T. 1583, 828 U.N.T.S. 305, recentemente emendate il 28 settembre 1979.

[59] R.C. Dreyfuss, *An Alert to the Intellectual Property Bar: The Hague Judgments Convention*, in *University of Illinois Law Review*, 2001, pp. 421, 423.

[60] Paris Convention, *op. cit.*

[61] Convention Establishing the World Intellectual Property Organization, July 14, 1967, 21 U.S.T. 1749, 828 U.N.T.S. 3.

[62] Id.

[63] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197.

[64] "Article 39. 1. In the course of ensuring effective protection against unfair competition as provided in Article 10-*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.; 2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, gener-

protezione "against unfair commercial use"[65]. L'accordo, quindi, protegge i segreti commerciali, non come proprietà intellettuale individuale, bensì come divieto di concorrenza sleale e fornisce un sistema di composizione delle controversie, il Dispute Settlement Body[66]. Ed ancora, consente "criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed willfully and on a commercial scale". Il TRIPS, va tuttavia segnalato, riconosce agli Stati membri un'ampia possibilità di derogare ai propri obblighi, permettendo loro di adottare leggi interne contrarie agli impegni dell'accordo quando volte a proteggere "sectors of vital importance to their socio-economic and technological development, which may allow countries to avoid specific prohibitions against economic espionage"[67].

7. Quanto alla responsabilità degli Stati in materia di spionaggio economico, ricordato che tale responsabilità si estende anche alle azioni degli Stati commesse nel cyberspazio, il citato Manuale di Tallin ha riconosciuto che "a victim state is entitled to take proportionate measures to end harmful ongoing cyber operations if the state of origin fails to meet its obligations to end them"[68]. Lo Stato leso, e solo questo, può ricorrere a contromisure se in presenza di una violazione di un obbligo internazionale e se l'atto illecito può essere attribuito allo Stato attore[69]. Per stabilire la responsabilità dello Stato per atti di spionaggio economico e pertanto intendere questi come atti illeciti commessi da uno Stato, non è sufficiente qualificare tali atti

---

ally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.; 3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use".

[65] TRIPS Agreement, art. 39.

[66] Il DSB ha l'autorità di istituire gruppi di composizione delle controversie, deferire questioni all'arbitrato, adottare panel e relazioni arbitrali, mantenere la sorveglianza sull'attuazione delle raccomandazioni e delle decisioni contenute in tali rapporti e autorizzare la sospensione delle concessioni in caso di non conformità con quelle raccomandazioni e decisioni.

[67] TRIPS Agreement, art. 8.

[68] *Tallin Manual*, *op. cit.*, p. 29 ("a State bears international responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation").

[69] *Case Nicaragua v. United States*, § 249 ("The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts… They could not justify countermeasures taken by a third state…"); REPORT OF THE INTERNATIONAL LAW COMMISSION, 53rd Sess., Apr. 23–June 1 and July 2–Aug. 10, 2001, U.N. Doc. A/56/10; GAOR; 56th Sess., Supp. No. 10, § 68, 2001.

come una violazione di un obbligo giuridico internazionale; l'azione deve essere altresì attribuibile allo Stato alla luce del diritto internazionale[70].

Pochi sono i dubbi sul fatto che il furto delle informazioni riservate di proprietà di una società sia qualificabile come un atto di concorrenza sleale. L'art. 1, paragrafi 1 e 2 della citata Convenzione di Parigi, precisa che l'accordo è stato concepito per proteggere la proprietà industriale, comprensiva di "patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations of origin". Questo significa che gli atti di spionaggio economico contro la proprietà intellettuale, i segreti commerciali, i progetti e similari rientrano certamente nell'ambito della tutela offerta dalla Convenzione ed una loro commissione costituisce una violazione dell'art. 10-*bis*, così come novellato nel 1967.

8. In che modo gli Stati possono proteggere le loro aziende dallo spionaggio economico e quindi neutralizzare la minaccia alla sicurezza nazionale che esso rappresenta? Lo Stato vittima può invocare l'uso di contromisure le cui regole sono state delineate nel caso Naulilaa e successivamente elaborate dall'International Law Commission (*successivamente*, ILC)[71]. Le contromisure non possono comportare l'uso della forza, infrangere norme perentorie e non possono violare gli obblighi di rispettare l'inviolabilità degli agenti diplomatici e consolari[72]. Le azioni in risposta, è noto, devono anche essere proporzionate, ossia "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the

---

[70] REPORT OF THE INTERNATIONAL LAW COMMISSION, *op. cit*., art. 2(a).

[71] *Naulilaa Incident Arbitration* (Port. V. Ger.), 2 RIAA 1011, 1928, parr. 1025-26. Questa decisione è considerata la dichiarazione più autorevole in materia di diritto consuetudinario sulle rappresaglie. Nel 1947, l'Assemblea Generale delle Nazioni Unite ai sensi dell'art. 13.1.a diede vita all'International Law Commission con l'incarico "the promotion of the progressive development of international law and its codification". U.N.G.A. Res.174(II), U.N. GAOR, 2nd Sess., U.N.Doc. A/RES/174(II) (Nov. 21, 1947). Detto brevemente, le contromisure devono essere: "aimed at the state that violated its obligations towards the injured state; limited to the temporary non-performance of the obligations of the injured state and should as far as possible be reversible so as to allow for the resumption of the performance of the original obligation; terminated when the wrongdoing state has complied with its obligations; commensurate with the injury suffered and have as their purpose to induce the wrongdoing state to comply with its obligations under international law". Rep. of the Int'l Law Commission, *op. cit.*, artt. 30,31, 49, 51, 53; sulla proporzionalità, Franck suggerì che "in assessing the acceptability of a response, the principle of proportionality allows those affronted by unlawful conduct to respond by taking into account the level of response necessary to prevent recurrences". T. FRANCK, *On Proportionality of Countermeasures in International Law,* in *American Journal of International Law*, vol. 102, 2008, pp. 765-766.

[72] Il punto che le contromisure non possano comportare l'uso della forza è stato contestato da diversa dottrina ed anche da parte della Corte Internazionale di Giustizia. Ad esempio, il Giudice SIMMA, nel suo parere sul caso *Oil Platforms* precisò che in determinate circostanze uno Stato può ricorrere a contromisure implicanti l'uso della forza. Oil Platforms Case (Iran v. U.S.), Separate Opinion of Judge Simma, 2001 I.C.J. 333 (Nov. 6). Per gli altri divieti, vedasi REPORT OF THE INTERNATIONAL LAW COMMISSION, *op. cit*., art. 50(1)(b), 50(1)(c); UNGA Res. 56/83, par.2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, Jan, 28, 2002, art. 50(2)(b).

rights in question"[73]. Questo tipo di proporzionalità, tuttavia, si distingue dal requisito di proporzionalità per le azioni di legittima difesa in risposta agli attacchi armati[74]. Mentre le azioni degli Stati in risposta od in previsione di un attacco armato, non devono superare la quantità di forza necessaria per fermare la minaccia[75], le contromisure intraprese per contrastare per un'azione illecita devono essere equivalenti al pregiudizio subito dallo Stato vittima[76]. Un approccio un po' più ampio è stato adottato, ad esempio, nel caso *Air Services*, incorporando nella valutazione della proporzionalità delle misure, una valutazione del diritto coinvolto nell'atto illecito, giungendo a dichiarare che "it is essential in a dispute between States, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principles arising from the alleged breach"[77]. La dottrina non si è mostrata unita sul fatto che soggetti privati possano ricorrere a contromisure per le lesioni subite da uno Stato[78]. Mentre le contromisure possono essere imposte solo dagli Stati alla luce del diritto internazionale, uno Stato leso ha il diritto di ricorrere alle capacità del settore privato per imporre con efficacia delle contromisure allo Stato offensore[79]. Tuttavia, pur facendo ricorso ai servizi di un soggetto privato per attuare le contromisure, lo Stato vittima si assume la responsabilità derivante da

---

[73] U.N.G.A. Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, art. 50(2)(a) (Jan, 28, 2002) art. 51.

[74] *Naulilaa Incident Arbitration*, *supra* note 332, at 1028. Rep. of the Int'l Law Comm'n, 53rd Sess., art. 51 commentary.

[75] Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 51.

[76] M. SCHMITT, *Cyber operations and the jus ad bellum revisited*, in *Villanova Law Review*, vol. 56, 2011, p. 19. Per illustrare come la proporzionalità delle contromisure nelle azioni in parola possa essere valutata, ricordiamo il caso dello spionaggio economico condotto dalla Cina (nel 2009) ai danni degli Stati Uniti. Nel caso in parola, il furto di proprietà intellettuale provocò (secondo un'analisi del Department of Commerce) una perdita di 27 milioni di posti di lavoro, con un valore di circa 48.2 miliardi di dollari in royalties e contratti di vendita persi ed in licenze. (ESA & USPTO, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: INDUSTRIES IN FOCUS (March 2012); China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, Inv. No. 332-519, USITC Pub. 4226 (May 2011) (Final)). Ancora più importante dell'impatto sull'occupazione e sul volume di affari, fu il suo effetto sul principio di concorrenza leale nel mercato globale considerato che il furto di proprietà intellettuale mina "both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and new industries that can further expand the world economy and continue to raise the prosperity of all". (D.C. BLAIR, J.M. HUNTSMAN, *The IP Commission Report: the report of the Commission on the theft of American Intellectual Property*, 2013, p. 10).

[77] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, art. 50(2)(a) (Jan, 28, 2002), art. 51.

[78] J.E. MESSERSCHMIDT, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, in *Columbia Journal of Transnational Law*, vol. 52, 2013, pp. 275, 276 ("States have an obligation of due diligence to prevent significant transboundary cyberharm to another state's intellectual property. Affected states may be entitled to reciprocate by…allowing their victimized nationals to hackback.").

[79] Z. WEST, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, in *Syracuse Law Review*, vol. 63, 2012, p. 119.

atti (eventualmente) illeciti commessi dalla società[80]. In altre parole, i soggetti privati sarebbero tenuti ad osservare i limiti stabiliti dal diritto internazionale per l'esecuzione delle contromisure.

Attualmente è evidente un'ambiguità tra il diritto consuetudinario e gli articoli dell'ILC sul quando inizi e quando finisca il diritto di attivare le contromisure. I requisiti di risoluzione delle controversie previsti dagli articoli dell'ILC sono tenuti separati da quelli richiesti per la fase anteriore e posteriore alle contromisure[81]. La dottrina che si opponeva ad includere un processo di risoluzione delle controversie prima del ricorso alle contromisure, riteneva che tale requisito avrebbe consentito allo Stato responsabile dell'illecito di apparire come aperto ai negoziati al fine di contrastare l'uso legittimo delle dette contromisure nei suoi confronti[82]. Così intesi, gli articoli proposti finirebbero per fornire allo Stato colpevole un sistema per evitare la sua responsabilità[83].

Alla fine, l'ILC omise dal testo finale qualsiasi procedura di soluzione volontaria od obbligatoria della disputa[84]. Viene chiesto allo Stato leso di denunciare l'illecito, proponendo il negoziato prima di ricorrere alle contromisure[85] ma gli articoli non richiedono che le parti avviino un negoziato prima che vengano attivate le contromisure[86]. Questi requisiti sono in linea con gli obiettivi delle contromisure ossia ritornare allo status quo ante la violazione ed impedirne la realizzazione.

Le contromisure, come prevedibili, devono essere sospese se l'illecito cessa oppure se la controversia penda dinanzi ad un tribunale, competente ad assumere

---

[80] *Tallin Manual*, *op. cit.*, p. 33. ("A state may not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.").

[81] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, (Jan, 28, 2002), artt. 52(1)(b), 43.

[82] D. BODANSKY, J.R. CROOK, D.J. BEDERMAN, *Counterintuiting Countermeasures,* in *American Journal of International Law*, vol. 96, 2002, pp. 817, 824.

[83] Un simile approccio è però stato respinto nel citato caso *Air Services Agreement* quando il Tribunale ha valutato l'intransigenza della Francia prima dell'applicazione statunitense delle contromisure, respingendo la necessità di esaurire tutte le procedure prima di ricorrere alle contromisure (Air Services Agreement Award (Fr. v. U.S.), 18 R.I.A.A. 416, 445 (1978) ("The Arbitral Tribunal does not believe that it is possible, in the present state of international relations, to lay down a rule prohibiting the use of counter-measures during negotiations, especially where such counter-measures are accompanied by an offer for a procedure affording the possibility of accelerating the solution of the dispute.").

[84] D. BODANSKY, J.R. CROOK, *Symposium – The ILC's State Responsibility Articles – Introduction and Overview*, in *American Journal of International Law*, vol. 96, 2002, p. 787 ("The proposed linkage between resort to countermeasures and compulsory dispute settlement was high controversial, not least because it permitted a target state to thwart the good-faith use of countermeasures through sham recourse to settlement procedures.").

[85] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, (Jan, 28, 2002), arts. 52(1)(b).

[86] ID.

decisioni vincolanti per le parti[87]. In alcune circostanze, gli effetti delle azioni illecite possono comportare un obbligo di riparazione e quindi la domanda è se lo Stato leso sia tenuto a cessare le contromisure prima che lo Stato offensore termini di pagare le riparazioni. Gli articoli dell'ILC non affrontano direttamente questo problema e sembrano dar vita ad un ostacolo assoluto al mantenimento in vita delle contromisure una volta che la condotta incriminata è cessata[88]. Questo sembra non essere in linea con quanto deciso nel caso *Air Services Agreement*: una volta che una disputa è sottoposta al tribunale che ha i "means to achieve the objectives justifying the counter-measures", il diritto di attivare contromisure risulta viziato e quelle già in vigore possono essere eliminate ma solo nella misura in cui il tribunale può fornire equivalenti "interim measures of protection"[89]. Il tribunale deve quindi avere l'autorità di ordinare "interim measures of protection, regardless of whether this power is expressly mentioned or implied in its governing statute (at least as the power to formulate recommendations to this effect)"[90]. Mancando tale autorità oppure se la sua capacità d'intervento è severamente limitata, lo Stato leso può mantenere in vita il diritto di iniziare o continuare le contromisure[91]. Al momento, i tribunali arbitrali internazionali non hanno ancora fornito sufficiente certezza agli Stati in merito alla loro capacità di applicare in modo efficace le misure provvisorie. Non è chiaro se i tribunali abbiano il potere di imporre misure provvisorie con la stessa efficacia delle contromisure adottate dagli Stati lesi. Molto probabilmente, anche alla luce della sentenza della Corte di Giustizia sul caso *LaGrand* sull'effetto vincolante delle misure provvisorie, i governi rimangono dubbiosi sul fatto che un sistema di misure provvisorie imposte da un tribunale possa essere realmente efficace quanto le contromisure[92].

Rimane la irrisolta questione relativa all'esaurimento delle controversie prima che si faccia ricorso alle contromisure, anche nell'ambito del WTO. In linea generale, non è possibile adottare contromisure quando la controversia è soggetta ad una procedura di risoluzione della stessa[93]. Questo è valido anche quando il meccanismo

---

[87] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, (Jan, 28, 2002), art. 52(3)(a); art. 52, cmt 7. ("Paragraph 3 is based on the assumption that the court or tribunal to which it refers has jurisdiction over the dispute and also the power to order provisional measures.").

[88] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, (Jan, 28, 2002), art. 52.

[89] Ancora, nel caso *Air Services*, fu osservato che "it is not possible, in the present state of international relations, to lay down a rule prohibiting the use of counter-measures during negotiations". Spetterà allo Stato leso valutare gli effetti dell'emissione delle contromisure contro le potenziali decisioni di un organismo internazionale. AIR SERVICES AGREEMENT AWARD, *op. cit.*, para. 96.

[90] ID.

[91] ID. ("As the object and scope of the tribunal to decide on interim measures of protection may be defined quite narrowly, however, the power of the Parties to initiate or maintain countermeasures, too, may not disappear completely.").

[92] *LaGrand* Case (Ger. v. U.S.), Judgment, 2001 I.C.J. 466 (June 27).

[93] UNGA Res. 56/83, para. 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, (Jan, 28, 2002), art. 50(2)(a).

di risoluzione delle controversie è contenuto nel trattato che lo Stato offensore ha violato[94]. In questo modo, gli Stati hanno volontariamente deciso di rinunciare al diritto alle contromisure quando firmano un trattato che include una procedura di risoluzione delle controversie. Mentre le disposizioni sulla risoluzione delle controversie del WTO possono imporre determinate restrizioni sui tipi di misure che uno Stato potrebbe adottare in risposta allo spionaggio economico, il dovere di uno Stato di non intervenire in un altro Stato per sottrarre proprietà intellettuale si è sviluppato come un distinto obbligo internazionale al di fuori dei trattati che gli Stati hanno firmato nel contesto del WTO. Da quanto detto, emerge un quadro abbastanza confuso sull'attuale sistema normativo delle contromisure e come si collochino nella fase di risoluzione delle controversie. Ad esempio, come possibile notare dalla lettura degli articoli dell'ILC, gli obblighi di preavviso e l'offerta di negoziazione potrebbero essere applicabili lì dove è ritenuto necessario il ricorso a contromisure urgenti per preservare i diritti dello Stato leso[95]. Come nel caso di un contesto cibernetico dove la velocità d'intervento è tutto[96]. Lo Stato leso deve quindi distinguere tra contromisure urgenti, che non richiedono preavviso, ed un'offerta di negoziazione e contromisure normali per le quali trovano applicazione i requisiti previsti dagli articoli dell'ILC. La sfida, forse, sarà sui panels arbitrali internazionali e se saranno in grado di trarre una simile distinzione quando la questione verrà loro sottoposta.

9. Ai fini della narrazione, rileva l'importante previsione contenuta nell'art. 10-*bis* della Paris Convention for the Protection of Industrial Property, nella sua revisione del 1967, ove si dispone che:

1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition.

2) Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.

3) The following in particular shall be prohibited:

a) all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor;

b) false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor;

c) indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods.

Il citato articolo, solleva tre questioni. Prima di tutto, lo spionaggio economico è un "*act of competition*"? Nella sentenza SKF v Jordan (1988), la Commissione

---

[94] Jurisdiction of the ICAO Council (India v. Pak.), Appeal, I.C.J., para. 16, 1972.

[95] ID., art. 52(2).

[96] M.SCHMITT, *Cyber Operations, op. cit.*, p. 14.

della Comunità Economica Europea stabilì che la definizione di "atto di concorrenza", ai sensi dell'art. 10-*bis*, para. 2, include solo i comportamenti condotti dai "concorrenti"[97]. Se questa interpretazione fosse corretta, lo spionaggio economico non può essere ritenuto come un atto di concorrenza in quanto lo Stato che modifica la norma non è un concorrente della società ritenuta lesa. Un'interpretazione della vicenda, forse migliore perché più ampia, vorrebbe che un atto di concorrenza non dipenda dagli attori coinvolti nell'attività denunciata, concentrandosi invece sull'impatto di tale attività sui partecipanti nel mercato (e quindi ci si chiede se una data società è o meno svantaggiata dal comportamento dell'altra).

È questa un'interpretazione decisamente da preferire perché in linea con l'oggetto della Convenzione di Parigi ossia di prevenire la concorrenza sleale – in generale – all'interno dell'Unione piuttosto che tra concorrenti all'interno dell'Unione stessa (art. 1). Seguendo questo approccio, lo spionaggio economico sarebbe un "atto di concorrenza" in quanto minerebbe il vantaggio competitivo di una società "target". La seconda questione emergente è se considerare lo spionaggio economico

---

[97] Decisione della Commissione del 23 dicembre 1988 che respinge il ricorso presentato dalla società Smith Kline & French Laboratories Limited nei confronti della Giordania, in base al regolamento (CEE) n. 2641/84 del Consiglio (89/74/CEE) - Gazzetta ufficiale n. L 030 del 01/02/1989, pp. 67,68. La società di diritto inglese, Smith Kline & French Laboratories Ltd, produceva ed esportava in Giordania un prodotto (il Tagamet), la cui sostanza attiva era la cimetidina, sviluppata dal polimorfo nuovo, di cui la Smith Kline ne era inventrice. Alla Commissione fu presentata denuncia dalla Smith & Kline secondo la quale la Giordania, emanando una legge (la n. 8 del 1986), modificante la legge sui brevetti del 1953, di fatto avrebbe privato la ricorrente della protezione garantitale precedentemente dal brevetto del polimorfo nuovo, violando così gli artt. 10-*bis* e ter della Convenzione di Parigi. Secondo la denuncia, la Giordania si sarebbe resa colpevole di una pratica commerciale illecita, causando un pregiudizio rilevante all'industria. Quanto alla violazione dell'articolo 10-*bis*, paragrafo 1, la società afferma che l'adozione della legge n. 8 costituirebbe, nel caso della Giordania, "un atto di concorrenza sleale" ai sensi di tale disposizione, in quanto sopprimendo in parte, per quanto si riferisce ai prodotti farmaceutici, la tutela dei brevetti, che la legge del 1953 attribuiva precedentemente alle invenzioni brevettate, essa avrebbe consentito ad operatori economici concorrenti di trarre vantaggio, senza alcuna contropartita, dagli investimenti effettuati da altri operatori economici, il che sarebbe contrario agli usi leali in materia industriale e commerciale. Aggiunge che la modifica legittimerebbe gli atti di concorrenza sleale che sarebbero stati commessi dai concorrenti prima della modifica della legge. Quanto alla violazione dell'articolo 10-*ter*, con l'adozione della legge n. 8 del 1986, la Giordania, "non garantirebbe più i rimedi giuridici adeguati per reprimere efficacemente" gli atti di concorrenza sleale, contravvenendo così a tale disposizione. La pratica commerciale, presuntivamente, illecita avrebbe comportato un pregiudizio rilevante all'industria perché le avrebbe impedito, di fatto, di smerciare i propri prodotti in Giordania e sugli altri mercati arabi, subendo un danno di almeno 480 mila sterline all'anno. La Commissione dichiarò non ricevibile la domanda presentata dalla Smith & Kline in quanto, non sufficientemente provata ai sensi dell'art. 3 para. 2 del regolamento CEE n. 2641/84. Infatti, visto che il para. 1 dell'art. 10-*bis* non definisce la nozione di atto di concorrenza sleale, viene ricordato che possono rientrare in tale nozione solo gli atti compiuti dai concorrenti, senza comprendere in essi anche gli atti legislativi di uno Stato firmatario. Infine, visto che l'art. 10-*bis* non impone uno standard minimo di protezione effettiva in materia di brevetti, la circostanza che uno Stato revochi con effetto retroattivo la tutela che la sua precedente normativa riconosceva a prodotti (farmaceutici nel caso di specie) stranieri, non costituisce una violazione di questa disposizione.

come un atto di concorrenza sleale. Quest'ultima è definita dall'art. 10-*bis*, para. 2, come "any act of competition contrary to honest practices in industrial or commercial matters". Il successivo paragrafo 3 fornisce tre esempi di concorrenza sleale, nessuna di queste include il furto di informazioni commerciali precisando però che l'elenco delle attività che costituiscono di concorrenza sleale, non è esaustivo, incoraggiando un'interpretazione estensiva del concetto di concorrenza sleale visto che parliamo di qualsiasi atto "contrary to honest business practices".

Ancora. L'articolo 10-*bis* impone obblighi extraterritoriali? Parte della dottrina sostiene che l'ambito di applicazione dell'art. 10-*bis* sia limitato dal punto di vista territoriale perché impone agli Stati di proteggere i cittadini degli Stati firmatari della Convenzione, da atti di concorrenza sleale, quando fisicamente situati all'interno del loro territorio. Così dicendo, viene esclusa l'applicazione dell'art. 10-*bis* allo spionaggio economico in quei casi in cui uno Stato rubi informazioni di proprietà di società private situate all'interno di giurisdizioni straniere.

Al momento, non esiste giurisprudenza o prassi statale sul fatto che l'articolo in parola non imponga obblighi extraterritoriali agli Stati[98]. Come può uno Stato vittima a far rispettare l'art. 10-*bis*? La Convenzione di Parigi non è inclusa nel WTO e di conseguenze, le presunte violazioni dell'accordo non possono essere perseguite dall'organo di composizione delle controversie del WTO. Tuttavia, gli artt. 1, 12 e 19 della Convenzione di Parigi, nella sua revisione del 1967, sono stati introdotti nel WTO dall'art. 2.1 del TRIPS del 1994. In ragione di ciò, l'art. 2.1 consente allo Stato membro del WTO di invocare la valutazione del gruppo di esperti per discutere dell'eventuale violazione dell'art. 10-*bis* da parte di un altro Stato membro del WTO.

10. Anche se una specifica norma che vieti lo spionaggio economico non è ancora in esistenza, gli Stati, come visto precedentemente, possono fare ricorso a contromisure per fermare l'intervento di un altro Stato, in quanto coerenti con i valori riconosciuti dalla comunità internazionale senza violare la *domestic jurisdiction* dello Stato offensore. Di certo, l'attività di *intelligence* può efficacemente tutelare l'ordine pubblico, incentivare la cooperazione, promuovere la pace, ridurre le tensioni internazionali giungendo anche ad indicare di quali norme il diritto internazionale dovrebbe dotarsi in materia[99]. Tuttavia, lì dove la competizione economica non pone

---

[98] C.J. TAMS, A. TZANAKOPOULOS, A. ZIMMERMANN, *Research Handbook on the Law of Treaties*, Elgar, Cheltenham, 2014.

[99] Al pari dello spionaggio "tradizionale", non vi è alcun divieto giuridico per la pratica dello spionaggio informatico. Trattasi di una forma, non meno invasiva e non meno devastante, di spionaggio che non raggiunge il livello di "uso della forza" o di attacco armato (eventi previsti e sanzionati dal diritto internazionale). Visto che gli obiettivi degli esperti di spionaggio informatico sono gli stessi di quelli ricercati dallo spionaggio tradizionale (l'acquisizione di informazioni riservate), cambiando solo nei mezzi e nelle modalità praticate, parte della dottrina sostiene la similitudine dello status tra i due tipi di spionaggio. D.B. SILVER, *Intelligence and Counterintelligence*, in *National Security Law*, 2005, pp. 935, 965; B. DROGIN, *Russians Seem to Be Hacking Into Pentagon*, in *Los Angeles Times*, Oct. 7, 1999; B. GRAHAM, *Hackers Attack Via Chinese Web Sites*, in *Washington Post*, Aug. 25, 2005; A. LEWIS,

limiti al modo con il quale l'intelligence può essere utilizzata, lo sviluppo e l'evoluzione del diritto internazionale per regolamentare la competizione economica nel cyberspazio[100] saranno importanti per comprendere il comportamento degli Stati e fornire stabilità al sistema economico internazionale. Rimane in sospeso come gli Stati interessati dal fenomeno dello spionaggio economico possano efficacemente rispondere al furto di proprietà intellettuali a mezzo del cyberspazio e contrastare lo spionaggio economico. Alcuni hanno suggerito il ricorso a sanzioni economiche (come già avvenuto nelle relazioni economiche tra gli Stati Uniti e la Cina)[101], altri ancora hanno raccomandato un ruolo di maggior rilievo per il WTO quale forum mondiale per contrastare (d'intesa) il cyber spionaggio[102]. Va anche precisato che su questo ultimo aspetto, i contrari hanno non solo sottolineato l'incapacità del WTO di contrastare il fenomeno in parola[103] quanto l'esiguo interesse mostrato dal forum verso un ruolo di soggetto normatore e controllore[104]. Fermo quanto sopra, va detto che gli Stati ritengono sufficientemente efficace, per contrastare lo spionaggio economico, la normativa penale nazionale. Tuttavia, l'utilità del quadro normativo nazionale viene compromessa dalla circostanza che gli Stati avvertono come difficile (ed in particolare nel caso del cyber spionaggio economico) esercitare la loro giurisdizione sulle spie, visto che, appunto, hanno tenuto la condotta illecita da remoto senza mai entrare fisicamente nel territorio dello Stato vittima[105]. Emerge chiaro che il più grande difetto dei meccanismi di prevenzione agli atti di spionaggio è la loro

---

The Cyber War Has Not Begun, in CSIS, Mar. 2010, in www.csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf; M.S. McDOUGAL, *The Intelligence Function and World Public Order*, TEMP. L.Q., vol. 46, 1973, p. 432; C.D. BAKER, *Tolerance of International Espionage*, in *American University International Law Review*, vol. 19, 2003, pp. 1091, 1097; L.K. JOHNSON, *Think Again: Spies*, in Foreign Policy, Sept. 1, 2000, in www.foreignpolicy.com/articles/2000/09/01/ think_again_spies.

[100] Per un approfondimento, N. MELZER, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, 2011, www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

[101] D. CARDWELL, *Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying*, in N.Y.Times, Sept. 1, 2014, www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html.

[102] R.A. CLARKE, *A Global Cyber-Crisis in Waiting*, in Washington Post, Feb. 7, 2013, www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html ("Victims of Chinese economic espionage should seek to establish clear guidelines and penalties within the World Trade Organization system."); *China-Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, in World Trade Organization ww.wto.org/english/tratop_e/dispu_e/cases_e/ds362_e.htm.

[103] D.P. FIDLER, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, in *American Society International Law*, vol. 17, 2013, p. 2.

[104] ID., p. 3.

[105] Molto completo e puntuale il lavoro in chiave comparatistica condotto da M. REID, *A comparative approach to economic espionage: is any nation effectively dealing with this global threat?*, in *University of Miami Law Review*, vol. 70, 2016

efficacia incoerente o parzialmente tale. La natura stessa dello spionaggio è particolare ossia di atto segreto e questo spesso significa che il danno apparente è ben inferiore a quello effettivo. Le sanzioni, anche se applicate, possono essere eluse da quei paesi che rivestono una posizione di primo piano nel mercato internazionale, diminuendo, così, notevolmente le conseguenze per loro[106]. Inoltre, un organismo internazionale quali la Corte Internazionale Penale non ha giurisdizione in materia di spionaggio e forse potrebbe mostrarsi non interessata ad averla. Per queste ragioni, le contromisure sembrano essere il modo migliore per contrastare lo spionaggio purché supportate dagli organismi internazionali a partire dal Consiglio di Sicurezza delle Nazioni Unite.

Economic espionage in international law

Abstract: *Can an espionage act constitute interference in the internal affairs of a State? Furthermore. How can States protect their companies from economic espionage and thus neutralize the threat to national security it represents? The consequences of this real economic war, much more competitive and more subtle than the "traditional" one, are devastating: from the destabilization of the market to the failure of companies to mass unemployment up to the forced relocation of national companies. At present, there is no international treaty specifically governing economic espionage; while there are different conventions and agreements that prohibit actions deemed harmful to international trade or economic development. The Paris Convention of 1883 was the first international agreement aimed at protecting intellectual property, requiring the signatory nations to extend the protection of intellectual property provided to their citizens to foreign citizens, establishing uniform rules on the rights deriving from that property. Although the Paris Convention does not*

[106] Come esempio può essere preso in prestito il caso della reiterata violazione di proprietà intellettuale da parte della Cina ai danni degli Stati Uniti, nonostante la firma di un accordo tra le parti risalente al 2015. In risposta a tale rinnovato comportamento illecito, gli Stati Uniti potrebbero (e risulterebbe poi difficile negarne la legittimità) sviluppare ed applicare un sistema di sanzioni (come poi puntualmente avvenuto), sanzionare le imprese che beneficiano dello spionaggio economico effettuato tramite la rete internet e rafforzare il sistema di controspionaggio sviluppando e finanziando imprese statunitensi abili a contrastare le azioni di hackeraggio cinese. Quali sono le ragioni che hanno spinto la Cina a violare l'accordo sulla proprietà intellettuale? Probabilmente due. La prima è che Pechino, forse, non avrebbe mai avuto intenzione di abbandonare del tutto il cyber-spionaggio, intravedendovi l'opportunità di ottenere un vantaggio diplomatico nell'attuare i cambiamenti che già aveva in programma. Questo condurrebbe a ritenere che la Cina, in realtà, ha sempre avuto l'intenzione di continuare sulla strada dello spionaggio economico, magari riducendo i rischi nell'essere scoperta. La seconda ragione del ritorno all'hackeraggio industriale potrebbe consistere in una reazione alle crescenti tensioni politiche e commerciali tra gli Stati Uniti e Pechino. Infatti, dinanzi all'inasprimento da parte dell'amministrazione Trump nei confronti degli investimenti cinesi nei settori ad alta tecnologia, con blocco dell'attività delle società di telecomunicazioni e l'imposizione di dazi doganali contro le imprese cinesi che esportano negli Stati Uniti, la Cina potrebbe dimostrarsi poco interessata ad onorare l'accordo.

explicitly deal with economic espionage, Article 10 on unfair competition prohibits "any act of competition in industrial or commercial matters". Even if a specific rule prohibiting economic espionage is not yet in existence, states can resort to countermeasures to stop the intervention of another state, as they are consistent with the values recognized by the international community without violating the domestic jurisdiction of the offending State. Certainly, the intelligence activity can effectively protect public order, encourage cooperation, promote peace, reduce international tensions and even indicate which rules international law should have in this area. However, where economic competition does not limit the way in which intelligence can be used, the development and evolution of international law to regulate economic competition in cyberspace will be important to understand the behavior of states and provide stability to the international economic system. The penalties, when applied, can be circumvented by those countries that have a leading position in the international market, thus considerably reducing the consequences for them. Furthermore, an international body such as the International Criminal Court has no jurisdiction over espionage and may perhaps not be interested in having it. For these reasons, countermeasures seem to be the best way to counter espionage as long as they are supported by international bodies starting with the United Nations Security Council.

Keywords: *Economic espionage; World Trade Organization; International Law Commission; General Agreement on Trade and Tarifs; Trade-Related Aspects of Intellectual Property Rights Agreement; World Intellectual Property Organization; Paris Convention for the Protection of Industrial Property.*