La guerra dell'informazione e i nuovi equilibri internazionali: aspetti giuridici, tecnologici e geopolitici

Presentazione

Giovanni Ziccardi*

Foreword

Abstract: The forum, and the following contributions, concern the very current topic of information warfare. This is a subject that requires legal, technological, sociological, geopolitical and international analysis. The aim is to try to understand the nature (and the limits) of this type of war that, in the information society era, is connoting our society.

Keywords: Information warfare, Hacking, Social network, Disinformation, Information society.

Il tema delle guerre dell'informazione suggerisce, allo studioso, diverse linee di ricerca. Si prospettano, *ictu oculi*, questioni che toccano la geopolitica e le relazioni internazionali, problemi di diritto pubblico e di diritto internazionale, aspetti informatico-giuridici e nodi, da sciogliere, puramente tecnologici. Il tutto contribuisce a tratteggiare un quadro che non solo è di difficile interpretazione, ma che muta molto rapidamente (sia a causa dei cambiamenti politici, sia a causa dell'evoluzione digitale).

Nel presente Forum, studiosi di diversa estrazione (esperti di diritto, di geopolitica, di scenari internazionali e di tecnologie) forniscono alcuni suggerimenti di approfondimento su argomenti che stanno rendendo di grande attualità il problema della regolamentazione di uno "spazio elettronico" che sta rivestendo, nella vita sociale, sempre più importanza. Tali spunti di discussione si sono sviluppati nelle attività di ricerca quotidiane all'interno del Centro di Ricerca Coordinato in "Information Society Law" del Dipartimenti di Scienze Giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano e nel corso di un convegno sull'*information warfare* tenutosi nel maggio scorso.

* Professore associato di Informatica giuridica, Università degli Studi di Milano.

Il primo tema di discussione, come prevedibile, riguarda la guerra tra Stati e, soprattutto, come sia cambiato il rapporto di forza (e militare) a causa delle cosiddette "guerre tecnologiche" (*information warfare*).

L'asimmetria della tecnologia ha mutato completamente il quadro cui ci si era abituati. La prima esigenza tradizionale in una guerra – avere un esercito professionale, ben armato e numeroso – è stata sostituita dalla necessità, ormai indifferibile, di competenze informatiche che possono essere anche in capo a piccoli gruppi di individui capaci, comunque, di attaccare con efficacia un altro Stato. *Asimmetria*, quindi, intesa come nuova possibilità dei "Davide contro Golia": piccoli eserciti elettronici che possono sconfiggere intere Nazioni.

Un panorama simile ha portato a un aumento imprevisto di "attori" con nuove, e preoccupanti, potenzialità offensive. Anche Stati che, dal punto di vista dell'esercito "fisico" e delle forze da poter mettere in campo, non erano tenuti in considerazione come possibili fonti di minaccia, ora sono diventati attori primari del nuovo campo di battaglia elettronico.

Purtroppo il quadro degli eserciti elettronici oggi esistenti è molto sfumato, e non è facilmente individuabile così come si può fare con quello degli eserciti tradizionali. Accanto a Stati, come la Cina, che fanno vanto del proprio esercito elettronico (pur mantenendone riservati tanti aspetti), ci sono molte Unità militari che sono volontariamente tenute segrete, e ciò è possibile grazie, si diceva, alle piccole dimensioni. Ciò impedisce di fare una reale "mappa" degli eserciti elettronici o, comunque, di formazioni paramilitari o paragovernative che operano in questo ambito.

Le guerre elettroniche hanno, poi, posto il problema della *attribuzione* delle azioni belliche e della riconoscibilità (o meno) di un attacco informatico per, poi, qualificarlo come atto di guerra tra Stati.

Il primo problema, quello della "paternità" (*attribution*), è molto spinoso da risolvere. Mentre un atto offensivo bellico tradizionale – ad esempio: un missile lanciato su un ospedale – è molto facile da individuare, anche per i suoi immediati e visibili danni fisici, un attacco elettronico è molto più subdolo, difficile da percepire, quantificare e attribuire a un soggetto. Il caso di *Stuxnet*, citato nell'articolo di Angelica Bonfanti, è estremamente significativo: pur essendo chiara, sulla carta, la paternità del *malware* che ha attaccato la centrale nucleare iraniana (programmato dagli Stati Uniti d'America e da Israele), risulta estremamente difficile, analizzando il codice e le azioni d'attacco, attribuire una paternità certa all'azione e ai mandanti. Un attacco elettronico di questo tipo può non solo colpire infrastrutture critiche ma, anche, trafugare segreti industriali o cercare di alterare gli equilibri elettorali di una nazione. Le interferenze portate da criminali informatici russi contro la campagna presidenziale di Hillary Clinton nel 2016 sono un esempio di una simile minaccia concreta di cui non si conosce ancora con precisione la portata. Operare con strumenti di anonimizzazione o completamente automatizzati – ad esempio *bot* – rende fumosa la possibilità di collegare ogni azione a un'entità ben definita.

Un ulteriore aspetto è altrettanto delicato, e viene puntualmente affrontato nel Forum dai vari Autori: esistono azioni offensive elettroniche che non generano l'impatto devastante di un tipico attacco militare ma che sono in grado, comunque, di for-

nire un *vantaggio competitivo* all'attaccante e di colpire nel profondo le infrastrutture di uno Stato. L'attacco elettronico ai sistemi di informazione, di trasporto, di energia, al settore pubblico e sanitario di una Nazione può causare milioni di vittime. Come può, allora, il diritto cercare di disciplinare un aspetto così innovativo potendo contare su un quadro giuridico che, nella maggio parte dei casi, ha ancora in mente (e nelle norme) un "diritto di guerra" ancorato a un'idea tradizionale del conflitto bellico?

Un ulteriore tema trattato nel Forum, soprattutto nelle righe dei contributi di Giulio Terzi di Sant'Agata–Francesca Voce e di Fabio Rugge, è lo stretto collegamento intercorrente tra il quadro politico attuale, la guerra dell'informazione e i nuovi equilibri statali e internazionali che si stanno generando. Le tradizionali distinzioni "a blocchi di potere" – eredità del post-Guerra Fredda e del sistema creato dalla NATO – stanno lasciando il posto a centri di potere differenti che si stanno adattando sempre meglio alla liquidità della società elettronica.

Ciò comporta un passo interpretativo ulteriore, ben illustrato nei contributi di Antonio Lamanna e di Gabriele Sufia, che coinvolge le mappe, la cartografia e l'idea di poter disegnare delle nuove linee di comunicazione grazie ai flussi di dati che attraversano le Nazioni, prendendo in considerazione le connessioni, i cavi sottomarini in fibra ottica e i satelliti. L'idea di riuscire a cristallizzare su (nuove) mappe un'entità così fluida quale il ciberspazio, che sfugge alla maggior parte delle definizioni, è molto affascinante, soprattutto se rapportata alla concezione tradizionale che abbiamo dell'idea di spazio, di confini e di luoghi fisici.

Ciascuno di questi aspetti è chiaramente connesso.

Non possiamo prescindere da una corretta collocazione geopolitica se, prima, non risolviamo le questioni giuridiche. Al contempo, però, le questioni giuridiche necessitano di una valutazione preliminare corretta del quadro tecnologico e delle nuove "mappe" del flusso dei dati e delle connessioni che stanno tracciando i (nuovi) confini del mondo moderno. Purtroppo, il diritto sembra, ancora una volta, arrancare rispetto alla tecnologia: le definizioni classiche mal si attagliano al nuovo quadro, e la natura internazionale – e globale – della rete sembra sempre più impermeabile a tentativi di regolamentazione che devono essere obbligatoriamente previsti, quasi sempre, su base locale.

Ultimo ma non ultimo, vi è l'appoggio, spesso non dichiarato, o la tolleranza, da parte dei Governi, verso le attività di gruppi di criminali informatici che operano al fine di alterare gli equilibri in altri Stati.

Si tratta di una connivenza pericolosa che ha, però, dimostrato come la guerra dell'informazione sui social network sia oggi considerata non solo come una vera e propria arma, ma come la strategia più importante per dominare questo campo utilizzando anche sempre di più lo strumento della disinformazione.