CyB

IL DILEMMA della CYBER INTELLIGENCE

Mario Caligiuri

Pur nella continuità della struttura portante del ciclo dell'informazione, la cyber intelligence potrebbe rappresentare un'area autonoma rispetto all'intelligence tradizionale, divenendo punto d'incontro e di confluenza di più àmbiti[1]. *Più che rappresentare l'evoluzione o l'aggiornamento di quella classica, l'intelligence cibernetica coniuga elementi che operano con logiche diverse: da un lato le tecnologie e dall'altro il fattore umano. Nella necessaria ricerca di una sintesi emergono nuove competenze e inedite professionalità. In tale quadro, la formazione diventa centrale per la definizione di* Data Scientist, *figura che si prevede sarà tra le più richieste nei prossimi decenni per fronteggiare la sovrabbondanza di informazioni – quasi esclusivamente digitali – e saper individuare quelle effettivamente utili.*

IL BISOGNO DI INTELLIGENCE

Non passa giorno in cui i media non invochino l'intelligence come strumento fondamentale per combattere il terrorismo, dimenticando che per tanti anni, e non solo in Italia, ci si è adoperati in ogni modo per depotenziare un servizio fondamentale per gli Stati, utilizzato in tutti i tempi e in tutti i Paesi. L'intelligence ha a che fare con la logica, l'intelligenza, la contestualizzazione, l'analisi, il discernimento: qualità tipicamente umane. Oggi, però, le informazioni sono galassie di galassie, originate attraverso le nuove tecnologie. Ormai ci si attende una trasformazione radicale nella quale, entro pochi anni, le identità virtuali supereranno quelle fisiche, ponendo agli Stati la gestione di due distinte politiche[2]. Si stima che nel 2020 gli apparecchi elettronici collegati a internet saranno 50 miliardi, praticamente cinque volte la popolazione mondiale[3], e che il 91% delle economie dei Paesi avanzati e il 69% di quelli in via di sviluppo dipenderanno da internet[4]. È quindi evidente che il cyberspazio sarà l'àmbito della guerra e della politica estera, delle indagini giudiziarie e delle attività economiche, così come

1. Tra questi, anche la Social media intelligence (Socmint). Vedi Bonfanti 2015, pp. 237-268.
2. Schmidt – Cohen 2013, pp. 25-93.
3. Kissinger 2015, p. 340.
4. Gori 2015.

della vita sociale e politica, culturale ed educativa. Questa quantità sterminata di informazioni pone almeno due problemi. Il primo è rappresentato dalla conoscenza inutile[5], nel senso che se non riusciamo a utilizzare le informazioni che abbiamo[6] la maggior parte di esse è priva di valore e complica ulteriormente la comprensione della realtà. Pertanto, diventa indispensabile la selezione, tecnologica e umana, volta a individuare le *relevant information* che effettivamente possano aiutare a comprendere e ad adottare le decisioni meno imperfette, nella consapevolezza che solo una porzione relativamente piccola di informazioni può risultare effettivamente utile. Il secondo aspetto è che la maggior parte dei dati e della conoscenza è nelle mani dei privati. Questa circostanza rappresenta una rivoluzione rispetto al passato, in quanto nella storia degli uomini le informazioni erano quasi tutte di proprietà di chi deteneva il potere, sia spirituale che temporale, mentre oggi lo sono di aziende private e, nello specifico, di colossi del web. Non a caso, gli uomini più ricchi del mondo sono i titolari di queste multinazionali, a dimostrazione della trasformazione dell'economia da materiale in immateriale.

IL TEMA DELLA COMPLESSITÀ

Viviamo in un mondo complesso. È stato sempre così, come ricordava anche John Locke nel XVII secolo, all'inizio della rivoluzione scientifica. E come ha sostenuto Stephen Hawking, «il ventesimo è stato il secolo della fisica, il ventunesimo è il secolo della complessità»[7]. Oggi questa complessità è aumentata con la globalizzazione, la tecnologia e l'evoluzione demografica che stanno modificando radicalmente e rapidamente l'ordine mondiale, ponendo questioni di varia natura, compreso il rapporto, talvolta inestricabile, tra economia legale ed economia criminale[8]. Le organizzazioni, di qualsiasi natura, diventano sempre più vaste e burocratizzate, mentre l'ambiente sociale diventa sempre più caotico con una proliferazione di informazioni e di attori. Di fronte a tale complessità, possiamo scegliere due strade: o ridurre quella interna o 'selezionare' quella esterna. La seconda via dovrebbe essere preferibile, sia per le aziende private che per le istituzioni pubbliche. Nell'individuazione della complessità esterna è fondamentale il ruolo dell'intelligence, inteso come metodo fondamentale per la gestione delle informazioni. Nell'era della complessità, la scienza dei dati e i big data (grandi dati) modificheranno «il nostro modo di vivere, di lavorare e di pensare»[9] generando «nuovo valore economico e d'innovazione»[10]. Con big data indichiamo l'enorme e complesso ammontare delle tracce digitali delle nostre attività quotidiane, come sottoprodotto della civiltà tecnologica in cui «il telefono, la radio, e soprattutto il computer consentono di tracciare chiunque e ovunque»[11]. I big data, intesi come l'insieme di dati personali e dei metodi per analizzarli, costituiscono uno straordinario microscopio sociale, uno strumento potente per la comprensione della società contemporanea. Nelle città, rese sempre più smart dai collegamenti digitali, aumentano le opportunità così come le vulnerabilità, i vantaggi al pari dei rischi. Semplicemente vivendo nel moderno mondo tecnologico, ciascuno di noi genera una marea di dati che restano nel web o vengono annotati da compagnie telefoniche e informatiche. Quando telefoniamo, preleviamo da un bancomat, acquistiamo un libro su Amazon, postiamo una foto su Facebook, esprimiamo un pensiero su Twitter, inviamo una email o un sms col nostro smartphone, o semplicemente navighiamo sul web, produciamo una grande quantità di tracce digitali, ognuna delle quali compone un piccolo pezzo del grande mosaico della nostra vita quotidiana. Queste tracce, i big data appunto, potrebbero offrire per la prima volta nella storia la possibilità di osservare le leggi che regolano il comportamento sociale, di comprenderlo e, in parte, anche di prevederlo. In questo contesto, la cyber intelligence (Cybint) diventa uno strumento prezioso per l'individuazione, la gestione e la valorizzazione delle informazioni, per riconoscere quelle che, di volta in volta, possano risultare importanti. Con riguardo all'utilizzo dei dati, per gli Stati, sia in via preventiva che successiva, è funzionale a garantire la sicurezza e il benessere ai propri cittadini mentre, per i privati, a inseguire legittimi profitti con le proprie attività. C'è però una terza, pericolosa casistica, che è rappresentata da chi intenda impiegare le informazioni per motivi illegali o immorali, per conseguire vantaggi illeciti, per truffare, ricattare, condizionare. A tale categoria sono riconducibili le organizzazioni criminali e terroristiche. Ma anche quelle legali, come Stati e imprese. I gruppi terroristici si avvalgono in modo sempre più consistente della rete e nel futuro «potrebbero impossessarsi di alcune tecnologie o disporre di fondi finanziari idonei ad accrescere la loro minaccia sulle infrastrutture critiche dei Paesi avanzati, ma non in misura tale da alterare le relazioni internazionali [...]. Diversa, invece, sarà l'evoluzione dell'attivismo hacker che, appunto, sarà sempre più comune online[12]. Le ragioni alla base dell'hacktivism saranno le più diverse e persino banali, ma la disponibilità in rete di molti strumenti digitali utili allo scopo attirerà un numero crescente di volontari. Queste stesse conclusioni si applicano al caso dello spionaggio online e del crimine informatico»[13]. Un discorso che si aggiunge a quello del cyber-oscuro (o deep web)[14], una dimensione ignota alla gran parte dell'opinione pubblica ma che contiene la stragrande maggioranza delle informazioni che viaggiano su internet[15]. Il deep web è un'area strategica per la Cybint, per l'evidente ragione che vi circolano notizie che non sono di dominio pubblico e rappresenta un àmbito popolato da organizzazioni terroristiche e criminali.

5. Il tema della conoscenza utile è un problema filosofico trattato anche da Aristotele, il quale definiva la conoscenza delle cose più importanti proprio nei termini della loro inutilità. Ed è proprio grazie a conoscenze 'inutili' che sopravvivono quelle utili. Il tema è stato affrontato da Ordine 2013.
6. Revel 1989.
7. Jogalekar 2013.
8. Shaxson 2012.
9. Mayer-Schönberger et al. 2013, p. 257.
10. Ivi, p. 24.
11. Levy 2001.
12. Secondo l'autore, si tratterà «più una forma di disturbo e fastidio [...] che altro anche in futuro», ivi, p. 250.
13. Ivi, pp. 250-251.
14. Teti 2015, p. 248.
15. Il «Journal of Electronic Publishing» nel 2001 ha diffuso una ricerca in cui ipotizzava che la dimensione oscura della rete fosse 500 volte maggiore dell'internet visibile.

L'espansione della rete richiama direttamente il tema della sua sicurezza, settore nel quale si stanno investendo cifre ingenti che, però, non garantiscono l'inviolabilità assoluta ai 2 miliardi di utenti di internet che inviano 294 miliardi di mail al giorno[16]. E a volte non è neanche una questione di denaro perché, secondo alcune fonti, la messa in rete di 11 milioni e mezzo di documenti relativi a investimenti nei paradisi fiscali – definita Panama papers – poteva essere evitata con una spesa di 6 euro e 13 centesimi, pari al costo di un comune programma informatico[17]. Come si può assicurare la sicurezza digitale? Nell'ordine, occorrono regole internazionali che preservino la riservatezza, investimenti sulla sicurezza delle tecnologie, sulla formazione continua degli operatori e sull'assicurazione dei rischi informatici che rappresenta un mercato in rapida evoluzione[18], in un contesto in cui le vittime spesso si accorgono in ritardo dei danni subìti.

LA NECESSITÀ DELLA DECISIONE

Stati, imprese e persone sono costrette, quotidianamente, a scegliere sulla base delle informazioni che hanno a disposizione. Nel 1955 l'economista Herbert A. Simon aveva elaborato la «teoria delle decisioni a razionalità limitata», nel senso che le scelte assunte tendevano a essere soddisfacenti e non ottimali, in quanto vi sono tre limiti con i quali confrontarsi: la parzialità delle informazioni a disposizione per decidere, i limiti delle capacità cognitive degli individui e l'esiguità del tempo a disposizione per scegliere[19]. Si decide in modo improvvisato e impreciso, e questa sembra essere una tendenza sostanzialmente universale[20]. La necessità della decisione richiede anche delle figure specifiche capaci di navigare con mano salda nelle acque perigliose del web per andare a individuare le informazioni giuste, nel tempo giusto e fornirle alla persona giusta. Tutto questo implica competenze informatiche, legate all'intelligenza artificiale e, in particolare, al *machine learning*: lo studio degli algoritmi che acquisiscono automaticamente gli schemi ricorrenti nascosti nei big data e creano modelli matematici; in altre parole si tratta di algoritmi che generano altri algoritmi. Le competenze informatiche, tuttavia, non bastano poiché occorre contestualizzare le informazioni, individuarle con sensibilità, collegarle in modo adeguato. Pertanto, l'intelligenza artificiale e quella umana devono andare di pari passo, perché quest'ultima è indispensabile per conferire profondità ed efficacia alla raccolta informativa, alla sua analisi e al suo utilizzo. In tale quadro il *data scientist* rappresenta una figura nuova di operatore con competenze multidisciplinari in grado di interpretare, trattare, analizzare e visualizzare i big data in modo

16. Cabinet Office Uk, *The Cost of Cyber Crime*: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf> [13 maggio 2016].
17. <ilgiornale.it/news/tecnologia/panama-papers-bastavano-sei-euro-fermare-furto-documenti-1244308.html> [13 maggio 2016].
18. *Assicurazioni cyber risk, un mercato in crescita*, «Cyber Affairs», Newsletter (11 aprile 2016).
19. Simon 1984.
20. Naim 2013.

efficace e opportuno. Ma, come evidenziava Robert D. Steele, una buona intelligence non serve in presenza di una cattiva politica[21], poiché le informazioni potranno essere anche le più efficaci, le più immediate e utili ma se chi deve utilizzarle non vi riesce, tutto il processo risulta inutile, anzi controproducente. Appunto per questo, la Cybint potrebbe rappresentare un'illusione, qualora venisse considerata la soluzione ai problemi dell'incapacità decisionale delle élite, che è invece il tema da porre con grande evidenza[22]. Infatti, all'intelligence si richiedono, da parte di decisori pubblici e privati, capacità interpretative e predittive degli avvenimenti in modo da poter assumere le decisioni conseguenti. Quello che conta non è la quantità delle informazioni ma la loro qualità. Va sempre ricordato che i dati devono trasformarsi in conoscenze capaci di illuminare le decisioni. Con la Cybint ciò diventa più probabile ma, nello stesso tempo, richiede maggiori competenze. Nello scenario futuribile che prospetta Jeremy Rifkin, nella sua società a costo marginale zero[23], ci potrebbe essere spazio non solo per le informazioni a nullo o bassissimo costo (come in gran parte avviene già oggi) ma anche per il loro trattamento, la loro estrazione e la loro valorizzazione. Questo potrebbe prefigurare una Citizen Cybint in analogia con la Citizen Intelligence, in cui non solo ogni cittadino è il produttore e l'utilizzatore delle proprie informazioni[24], ma anche un collaboratore delle autorità per la definizione delle politiche di interesse generale, a cominciare dalla sicurezza. Non a caso, nella progettazione delle smart city si prevede che l'applicazione delle tecnologie, unitamente ai rischi connessi, venga sperimentata con la diretta collaborazione dei cittadini[25]. Tale scenario si potrebbe anche prefigurare per la Cybint. Infatti, «gli individui saranno inevitabilmente costretti a prendere molto sul serio la propria difesa personale in rete, non delegandola esclusivamente allo Stato, alle Forze dell'ordine e ai militari, pena, in caso contrario, la perdita di informazioni e dati che sarà più difficile e costoso recuperare e/o ricostruire»[26]. Tanto più che nei prossimi anni «l'identità sarà il bene più prezioso di un cittadino, e la sua natura sarà principalmente online. I contatti con il mondo virtuale inizieranno sin dalla nascita, o magari anche prima»[27]. Questo aspetto postula un'opinione pubblica maggiormente informata verso gli scenari che vanno profilandosi e anche per rinsaldare il processo di fiducia tra Stato e cittadini per far fronte alle minacce alla sicurezza.

Un altro aspetto che non viene ancora adeguatamente affrontato, è l'integrazione delle fonti che provengono dai processi di Cybint con quelli originati dalla Humint, soprattutto se acquisiti da fonti chiuse o grigie. Questo per evidenziare come la particolare attività non sia affatto sempre sufficiente per assicurare un adeguato supporto informativo. Infatti, «la tecnologia da sola non è una panacea per i mali del mondo, ma il

21. Steele 2002.
22. Caligiuri 2008.
23. Rifkin 2015.
24. Teti 2013, pp. 69-89.
25. Caligiuri, *Intelligence: svelare le menzogne nella penombra dei big data*, «Aspenia online», 3.6.2015, <http://www.aspeninstitute.it/aspenia-online/article/intelligence-svelare-le-menzogne-nella-penombra-dei-big-data> [13 maggio 2016].
26. Foradori – Giacomello 2014, p. 251.
27. Schmidt – Cohen 2013, p. 32.

suo uso intelligence può fare la differenza»[28]. Occorre dunque evitare le illusioni decisionali affidando tutto alle procedure automatiche, come decenni fa aveva ben compreso il regista Stanley Kubrick, che con il D*ottor Stranamore* e 2001 O*dissea nello Spazio* aveva evidenziato una condizione non superabile che avrebbe condotto alla catastrofe. I recenti attentati di Parigi e Bruxelles, oltre a certificare un fallimento dell'intelligence, hanno evidenziato anche l'insufficienza della Cybint. Occorre avere la capacità di individuare obiettivi chiari e strategie efficienti che può essere ricondotta solo all'azione politica perché, in mancanza di questi, non ci sono tecnologie che bastino.

IL DILEMMA

Gli equilibri della scelta fra sicurezza e libertà rappresentano il dilemma della società contemporanea. Fino a che punto si può limitare la libertà individuale per garantire la sicurezza dello Stato? Non esiste una risposta buona per ogni occasione e per sempre. Per esempio, dopo gli attentati dell'11 settembre del 2001, l'amministrazione statunitense ha promulgato il Patriot Act, in base al quale venivano violate alcune garanzie individuali per difendere la Nazione dal terrorismo. Anche in questo caso la violazione della privacy è avvenuta e avviene attraverso modalità elettroniche e cibernetiche, con l'invadenza delle nuove tecnologie. Ma vi sono dei limiti, dovuti alla circostanza che, per la prima volta nella storia degli uomini, le informazioni sono quasi tutte sul web e sono possedute da imprese private. Quanto è accaduto tra la Apple e l'Fbi per l'acquisizione delle informazioni relative alla vicenda di San Bernardino è emblematico[29]. Solo apparentemente si tratta di contemperare le libertà individuali con le esigenze di sicurezza collettiva perché, in realtà, è una lotta di potere tra il settore pubblico e quello privato. È la punta dell'iceberg di uno scontro gigantesco che caratterizzerà sempre di più il futuro. In tale quadro la Cybint è fondamentale. Non a caso i governi stanno definendo politiche e investendo ingenti risorse per tutelare il cyberspazio: la Commissione Europea ha approvato nel 2013 la Cyber Security Strategy[30] e gli Stati Uniti nel 2016 hanno destinato al settore circa 15 miliardi di dollari, prevedendo inoltre l'assunzione di 6.000 esperti informatici[31].

CONCLUSIONE

Il dilemma della Cybint è particolarmente complesso. Da un lato, occorre coniugare la libertà individuale con la sicurezza collettiva e, dall'altro, è necessario integrare le competenze umanistiche con quelle scientifiche. La Cybint potrebbe, così, rappresentare un

28. Ivi, p. 323.
29. Il 2 dicembre 2015 a San Bernardino, in California, due terroristi, marito e moglie, hanno ucciso 14 persone, ferendone altre 23.
30. <http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm> [13 maggio 2016].
31. *The Pentagon Is Rethinking a $475 Million Cyber Defense Proposal*: <defenseone.com/ technology/2015/05/pentagon-rethinking-475-million-cyber-defense-proposal /113635 /?oref=search _cyber> [13 maggio 2016].

originale punto d'incontro per un recupero del rinascimento, dopo gli ultimi secoli bui segnati dalle ideologie che hanno provocato guerre e terrore, genocidi e fondamentalismi. È una speranza, ma anche una possibilità. E come per tutto quanto riguardi gli accadimenti del futuro, non si aspetta ma ci si prepara in un quadro in cui la cultura si è trasformata da conoscenza del passato in capacità di prevedere il futuro[32]. La Cybint potrebbe riuscire a fondere esigenze apparentemente diverse. E questo per non ridurla a un mero fatto tecnico, appannaggio di soli specialisti informatici o di esperti di big data: si tratterebbe di una visione estremamente riduttiva perché ogni azione umana avrà sempre bisogno di essere illuminata dal pensiero, strumento indispensabile per distinguere il segnale dal rumore e cioè le informazioni reali da quelle che invece le confondono. Spiega Nat Silver: «Fare una previsione ci è tanto difficile per la stessa ragione per cui è così importante: è il punto in cui la realtà oggettiva e quella soggettiva si intersecano. Riuscire a distinguere il segnale dal rumore richiede sia conoscenza scientifica, sia autocoscienza oltre alla serenità di accettare le cose che non possiamo prevedere, il coraggio di prevedere quello che non possiamo e la saggezza per riconoscere la differenza»[33]

32. Mayer-Schönberger et al. 2013, p. 257.
33. Silver 2013, p. 563.

BIBLIOGRAFIA MINIMA

M.E. Bonfanti, *Social media intelligence a salvaguardia dell'interesse nazionale*, in Gori – Martino (a cura di) 2015, pp.237-268
M. Caligiuri, *La formazione delle Élite. Una pedagogia per la democrazia*, Rubbettino, Soveria Mannelli 2008.
F. Foradori – G. Giacomello, *Sicurezza globale. Le nuove minacce*, il Mulino, Bologna 2014.
U. Gori – L. Martino (a cura di), *Intelligence e Interesse Nazionale*, Aracne, Roma 2015.
U. Gori, *Introduzione*, 6ª Conferenza annuale sulla Cyber Warfare, *Manovre Cyber: Impatto Sulla Sicurezza Nazionale* (Roma, giugno 2015).
A. Jogalekar, *Stephen Hawking's advice for twenty-first century grads: Embrace complexity*, «Scientific American blog» (23 Aprile 2013).
H. Kissinger, *Ordine Mondiale*, Mondadori, Milano 2015.
S. Levy, *Crypto: How the code rebels beat the government-saving privacy in the digital age*, Penguin USA, 2001.
V. Mayer-Schönberger – K. Cukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere. E già minaccia la nostra libertà*, Garzanti, Milano 2013.
M. Naim, *La fine del potere*, Mondadori, Milano 2013.
N. Ordine, *L'utilità dell'inutile*, Bompiani, Milano 2013.
J.F. Revel, *La conoscenza inutile*, Longanesi, Milano 1989.
J. Rifkin, *La società a costo marginale zero*, Mondadori, Milano 2015.
E. Schmidt – J. Cohen, *La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni*, Rizzoli Etas, Milano 2013.
N. Shaxson, *Le isole del tesoro. Viaggio nei paradisi fiscali dove è nascosto il tesoro della globalizzazione*, Feltrinelli, Milano 2012.
N. Silver, *Il segnale e il rumore. Arte e scienza della previsione*, Fandango, Roma 2013.
H. Simon, *La ragione nelle vicende umane*, il Mulino, Bologna 1984.
R.D. Steele, *Intelligence. Spie e segreti in un mondo aperto*, Rubbettino, Soveria Mannelli 2002.
A. Teti, *La 'Citizen Intelligence'. Intelligence del terzo millennio*, «Gnosis» 4 (2012).
A. Teti, *Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza*, Rubbettino, Soveria Mannelli 2015.