RESEARCH ANALYSIS
2017

CYBERSECURITY ED INTERNET OF EVERYTHING

PABLO MAZURIER

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

CYBERSECURITY ED INTERNET OF EVERYTHING

Pablo Mazurier

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

2017

RIGUARDO ALL'AUTORE

Pablo Andrés Mazurier è Phd in "Politics, Human Rights and Sustainability" alla Scuola Superiore Sant'Anna di Pisa con un progetto di ricerca in Internet Governance. E' stato ricercatore al King's College, University of London (UK) e all'Institut d'Études Européennes of the Université Libre de Bruxelles (Belgium). Ha ottenuto una Laurea Specialistica con lode in Studi Europei e Internazionali all'Università di Trento, con una tesi in "Sociology of Legal Regimes at the Global level", e una laurea in Giurisprudenza all'Austral University (Argentina).

CYBERSECURITY ED INTERNET OF EVERYTHING

1. L'alba dell'Internet of Everything

Internet fu originariamente pensata per condividere l'informazione. Poi, subì una rapida evoluzione migliorando ogni tipo di comunicazione umana come, ad esempio, rivoluzionando il commercio attraverso la digitalizzazione di ogni sua area. Con l'esponenziale crescita dei dispositivi mobili[1], delle applicazioni e dei social network, la nostra vita è completamente in rete, generando così una marea di dati[2] impossibili da controllare e gestire. L'ultima di queste sfide epocali è quella di connettere il resto degli oggetti che ci circondano dando vita al cosiddetto "Internet of Everything, massimizzando quindi il rapporto fra persone, processi, cose e dati.[3]

Questo cambiamento globale estremamente veloce[4] rappresenta non solo una rivoluzione in termini quantitativi ma anche in termini qualitativi[5], dato che non solo si genera molta più informazione sulle vite delle persone, ma si riescono a trovare anche nuovi parametri causali, nuove strade su come interpretare i comportamenti individuali – basate sulla neuroscienza, l'UX o scienza dell'esperienza degli utenti e le scienze cognitive con essenziale importanza per processi di partecipazione sociale quali i processi elettorali e la formazione dell'opinione pubblica. Questi sviluppi si ottengono

[1] In 1984 esistevano soltanto mille dispositivi collegati alla rete; un milione nel 1992; dieci milioni nel 2002; un miliardo nel 2008; dieci miliardi nel 2011. Mongay Batalla, J. et al. (eds.) (2017), p. 16. Cisco sostiene che ci saranno 26,3 miliardi di dispositivi collegati ad Internet entro il 2020, raggiungendo 200 miliardi se contiamo i microchip all'interno degli oggetti dell'Internet of Things. Rayes, A. and Salam, S. (2017), p. 26.

[2] Durante l'anno 2012 si sono generati più dati che in tutti i 5 mila anni prima. L'universo digitale attuale si duplica ogni due giorni. Turner, V. (2013). Ogni giorno il mondo produce circa 2 exabyte, cioè 2 miliardi di gigabyte. Dahir, H. (et al.) (2015), p. 12.

[3] Il nuovo internet connettera persone in modi più rilevante, trasformando dati in intelligenza per prendere decisioni migliori, offrendo informazione precisa per la scelta a persone e machine in tempo reale, e connetterà dispositive fisici e oggetti alla rete permettendo loro di prendere decisioni intelligenti. Rayes, A. and Salam, S. (2017), p. 3.

[4] Rayes sottolinea che la rata di adozione dell'Internet of Everything è cinque volte più veloce di quelle di crescita dell'elettricità e la telefonia. Rayes, A. and Salam, S. (2017), p. 23.

[5] Sulla base della legge di Metcalfe, che stabilisce che il valore di una rete di telecommunicazioni è direttamente proporzionale col quadrate del numero d'utenti collegati al sistema (n2). In alter parole, più dispositive e persone connesse, più valore avrà la rete.

attraverso l'uso complesso e congiunto di una serie d'innovazioni: Big Data, Cloud and Fog Computing, Analytics 3.0 e AI.

Big data consiste nell'estrazione e gestione di alti volumi di dati con alti gradi di complessità, che rendono estremamente difficile la pianificazione, raccolta, gestione ed analisi con metodi tecnologici tradizionali[6].

Per cloud computing[7] s'intende ogni servizio digitale consistente nell'accesso on-demand ad una rete contenente una vastità di risorse digitali condivise, rappresentando l'esempio del più recente modello di digitalizzazione o la virtualizzazione non solo del mondo, ma anche del rapporto materiale fra uomo e macchina. La "nuvola" non solo raccoglie i nostri dati, permettendoci di non avere necessità di supporti materiali come un hard disk, ma permetterà anche di caricare dati di traffico e gestione, superando la costruzione teorica basata nell'end-to-end principle.

La fog computing[8] è l'espansione del paradigma di cloud computing verso il basso, verso i più variegati e diversi oggetti e punti di raccolta dell'informazione, permettendo non solo una maggior raccolta di dati ma anche una connettività più elevata, ed il controllo direttamente dai punti di connessione in modo decentralizzato.

L'evoluzione verso Analytics 3.0[9] ci permette di, invece che raccogliere dati da diverse fonti ed inviarli tutti ad un punto centralizzato dove essi vengono sistematizzati e analizzati, realizzare l'analisi in vicinanza alla fonte, con la possibilità di operare procedure complesse in microsecondi senza necessità di traferire ingenti quantità di dati attraverso la rete.

L'AI ovvero l'intelligenza artificiale in realtà è un termine controverso, che si può definire indicando l'evoluzione delle macchine nell'acquisizione di capacità prettamente umane: da capacità analitiche per analizzare dati ed arrivare a conclusioni, fino a cogliere sfumature nel linguaggio, valutare comportamenti e attuare in autonomia. In questo percorso, molti scienziati e mass media si preoccupano per il punto d'arrivo, cioè l'ipotesi di coesistenza, in

[6] Kale, V. (2017), p. 208
[7] Kale, V. (2017), p. 177-8
[8] Dahir, H. (et al.) (2015), p. 13.
[9] Rayes, A. and Salam, S. (2017), p. 19.

genere conflittuale[10], fra umani e macchine super intelligenti in grado di attuare in autonomia e con un proprio livello di auto-coscienza e superiori capacità di memoria e analisi di dati. Tuttavia, molti dubitano di questo punto d'arrivo[11]. Al giorno d'oggi, l'AI è in grado solo di mettere assieme tutte le altre innovazioni elencate prima per offrirci un miglior livello di analisi e più complesse conclusioni su fenomeni naturali e sociali.

Grazie a tutte queste innovazioni messe insieme, l'IoE diventa *context-awareness*, in grado di offrire servizi automatizzati e contestualizzati per migliorare la qualità dell'esperienza dell'utente[12]. In questa nuova era della computazione cognitiva[13] le macchine non solo eseguiranno lavori specifici ma collaboreranno con gli uomini, inferendo conclusioni grazie ad un processo di gestione di dati più razionale, analitico e persino riflessivo.

Dipendendo dal tipo di connettività[14], la comunicazione M2P (da macchina a persona) cambierà radicalmente dato che l'informazione che le macchine provvedono agli utenti può essere automaticamente ed intenzionalmente manipolata, selezionata o persino nascosta in base al tipo di utente, alle sue preferenze e alle priorità con le quali è stato programmato il sistema attraverso l'uso di *Predictive Analytics*[15].

In questo modo, i dispositivi tecnologici saranno in grado d'incidere sulla percezione umana della realtà, aumentando le distorsioni e le tendenze individuali e sociali, essendo in grado persino di valutare le reazioni individuali sulla base di diversi "inputs". Nel recente dibattito sulla *post-verità* e la sua incidenza nella campagna elettorale

[10] Come sottolinea Good, "la prima machina ultraintelligente è l'ultima invenzione che l'uomo ha bisogno di fare, premesso che la machina sarà docile abbastanza per dirci come mantenerla sotto controllo." Good, I. J. (1965) Speculations concerning the first ultraintelligent machine, in Alt, F.L. and Ruminoff, M. (eds.) (1965), Advances in computers (vol. 6, pp. 31-88), Academic Press, London, cit. in Müller, V. C. (2016), Risks of Artificial Intelligence, CRC Press, Boca Raton, p. 3

[11] "AI doomsday scenarios belong more in the realm of science fiction than science fact". Ditterich and Horowitz (2015), Benefits and risks of artificial intelligence, cit. in Müller (2016), op. cit., p. 2.

[12] Mongay Batalla, J. et al. (eds.) (2017), p. 4

[13] Cognitive computing rappresenta una terza era della computazione, dopo i periodi del sistema tabulare e del sistema programmabile. Zomaya, A.Y. (2017), p. 814.

[14] L'IoE si basa in tre diversi tipi di collegamenti: M2M (macchina-a-macchina), M2P (macchina-a-persona) e P2P (persona-a-persona). Mongay Batalla, J. et al. (eds.) (2017), p. 8.

[15] Predictive analytics covers a large number of analysis techniques, including social media and geospatial analytics, Text mining and Sentiment analysis, which aims to identify, categorize and make presumptions of a user based on his/her relationships, everyday life habits, interests, opinion, priorities and hidden patterns discovered by applying big data analysis. Zomaya, A.Y (2017), p. 665.

statunitense, risulta evidente come le macchine e i dati riescono a distorcere la nostra percezione della realtà, dei rischi e dei problemi globali, generando un nuovo "toolkit" o "set" di vulnerabilità vincolate con l'ingegneria sociale.

La comunicazione M2M (macchina a macchina), usualmente chiamata l'Internet delle Cose, si riferisce alla connessione fra diverse tipologie di dispositivi, da sensori nel cibo fino ai freni delle auto, utilizzati per comunicare dati e prendere decisioni in modo autonomo senza intervento diretto umano. In questo *brave new world* della iper-storia[16], il centro di potere viene delocalizzato dal "vecchio" controllo diretto dell'uomo sull'uso delle cose, verso la scrittura del codice che andrà a regolare le azioni ed interazioni fra macchine, realizzate a livello micro, cioè grazie alla fog computing. Questo perché le grandi aziende tecnologiche e i governi stanno puntando fortemente sulla leadership nel settore[17].

2. Rischi per la Cybersicurezza

L'Internet of Everything presenta rischi sia tecnici che socio-politici in grado di essere usati da parte di cybercriminali e cyberterroristi.

Da un lato, in base alla definizione classica di rischio come una funzione fra minaccia, vulnerabilità ed impatto, l'IoE riguarda in particolar modo questi ultimi due elementi. La crescita dell'interconnessione fino ad arrivare a trilioni di connessioni[18] molte delle quali al suo *edge level*[19] dei sistemi di computazione *fog and cloud*, incrementando esponenzialmente la vulnerabilità di tutto il sistema, in particolar modo dalla più comune tecnica di attacco, il DDos ovvero il distributed denial-of-service[20], relativamente facile da portare avanti anche da parte di soggetti senza una grande

[16] Floridi, L. (ed.) (2015)
[17] "[I]n an era in which nation-bound laws regarding content no longer neatly comport with the globally dispersed and decentralized architecture of the global Internet, there is increasing recognition that points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the f low of money, information, and the marketplace of ideas in the digital sphere." Musiani, F. et al. (eds.) (2016).
[18] Mongay Batalla,J.etal.(eds.)(2017),p.4
[19] The connections at the edge level consist in physical devices and controllers (like sensors, machines, intelligent edge nodes of all types), programmed for several specific tasks and connected with the main network.
[20] Rayes, A. and Salam, S. (2017), p. 211.

conoscenza informatica, ma molto difficili di attribuire e abbastanza pericolosi da attirare l'attenzione dei social media e dell'opinione pubblica. La "nebbia" ubiqua conformata da sensori intelligenti, interconnessi, geo-localizzati richiede un alto livello di controllo e sorveglianza umana, rappresentando la parte più vulnerabile della società cibernetica del futuro. Inoltre, il livello d'impatto causato da un cyber attacco è direttamente proporzionale al controllo dei dispositivi lasciato all'AI per controllare la gigantesca quantità di dispositivi connessi in grado di controllare e gestire le più complesse situazioni della nostra vita quotidiana. Se l'unica soluzione possibile per assicurare questa transizione verso l'amministrazione dello *smart computing* è la fortificazione dell'internet, in realtà si miglioreranno soltanto le vulnerabilità tecniche, senza occuparsi di come combattere veramente le minacce, l'impatto ed il quadro più generale.

Per raggiungere soluzioni più ampie, l'ecosistema d'Internet dovrà centrare l'attenzione anche sul versante socio-politico della cyber sicurezza. Guardando il quadro generale, risulta essenziale mantenere un adeguato bilanciamento fra le tre dimensioni sociali del cyber spazio: internet, cyber conflitto e innovazione. Il rischio sistemico di frammentazione, l'erosione della fiducia collettiva ed il consenso, un'istituzionalizzazione incompiuta e la *balcanizzazione* dell'ecosistema cyber possono generare opportunità straordinarie per il cybercrime e cyber terroristi di esercitare la loro influenza e potere. Inoltre, mentre le aziende e i governi sono più preoccupati di dominare il cyberspazio ed ottenere benefici dall'innovazione che nel mettere in sicurezza i sistemi, queste minacce tenderanno a crescere.

La principale sfida per la comunità internazionale è il rafforzamento dell'intero sistema di sicurezza d'Internet, prevenendo che la logica della cyber guerra inquini l'ambiente di collaborazione, apertura e fiducia. Rafforzare i programmi di capacity-building regionali e locali, istituzionalizzare la governance multistakeholder e raggiungere un ampio e duraturo coinvolgimento del settore pubblico e privato sono i passi essenziali per eradicare le vulnerabilità. Dal 1998, tutti i governi statunitensi hanno chiesto una maggior collaborazione con il settore privato per rafforzare l'internet libero ed aperto e per promuovere un partenariato pubblico-privato su tematiche di cyber sicurezza. Tuttavia il settore privato, sebbene proprietario dell'85%

delle infrastrutture critiche nazionali[21], non ha voluto assumersi la responsabilità al posto dello Stato[22]. A questo punto, la dimensione continua ad essere un territorio fertile per l'insicurezza cyber[23], una situazione che paradossalmente porta benefici in modo indiretto sia all'industria dell'innovazione che al governo. Le aziende hanno potuto costruirsi delle "cyber fortezze", come le città stato medioevali, per mantenere gli utenti nelle loro sicure ma chiuse aree di controllo, e, dall'altra parte, i governi hanno potuto incrementare la loro legittimità nell'intervenzionismo sul cyberspazio per limitare gli abusi delle grandi aziende e industrie.

In un certo modo, ci troviamo di fronte ad una versione cyber della tesi già avanzata da Noreena Hertz[24], che sostiene che mentre i politici appena riescono a sopravvivere in un contesto di forti critiche e mancata fiducia da parte dei media e dei cittadini, le aziende sono in grado di offrire alle persone servizi informatici pubblici che i governi non sono in grado o non vogliono provvedere ad essere in grado di fornire. Come corollario di questa situazione, le grandi corporazioni hanno preso il controllo in modo silenzioso sui cittadini attraverso l'uso delle alte tecnologie, priorizzando i benefici economici e geopolitici sul rispetto e la promozione dei diritti individuali e dei valori democratici all' interno del dominio cyber. Il modello della cyber fortezza, con la sua limitazione alla privacy individuale e la mancata trasparenza e rendicontazione pubblica, porta ad un'inevitabile erosione della dimensione aperta, egualitaria e democratica di internet, che è essenziale per mantenere un adeguato sviluppo della società globale.

Un prospero futuro per la nostra società informatizzata dipende nel trovare il *medium virtus* in questa narrativa duale combinando il potere dello sviluppo tecnologico che promuove l'Internet of Everything, con il crescente potere distruttivo dei cyber attacchi.

[21] Carr, M. (2016), p. 101.
[22] Carr, M. (2016), p. 103.
[23] Governments and other actors are "*choosing to maintain a state of cyber insecurity*", Carr, M. (2016), p. 184.
[24] Hertz, N. (2003).

Bibliografia

• Ayala, L. (2016), *Cybersecurity Lexicon*, Apress, New York.
• Carr, M. (2016), *US Power and the Internet in International Relations*, Palgrave MacMillan, New York.
• Chen, T.M. et al. (eds.) (2014), *Cyberterrorism. Understanding, Assessment, and Response*, Springer, New York.
• Desouza KC, Hensgen T (2003), *Semiotic emergent framework to address the reality of cyberterrorism*, Technol Forecast Soc Change 70(4):388.
• Erikson, J. and Giacomello, G. (2007), *International Relations and Security in the Digital Age*, Routledge, London - New York.
• Gordon, S. and Ford, R. (2003), *"Cyberterrorism? Symantec Security Response White Paper"*, Cupertino.
• Hülsse, R. and Spencer, A. (2008), "*The Metaphor of Terror: Terrorism Studies and the Constructivist Turn*", in Security Dialogue, vol. 39, no. 6
• Kan, P.R. and Irwin J (eds)(2004), *War and virtual war: the challenges to communities*, Rodopi, Amsterdam.
• Lewis, J. A. (2002) "Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats", Centre for Strategic and International Studies (Online) http://www.csis.org
• McCarthy, D. (2015), *Power, Information, Technology, and International Relations Theory. The Power and Politics of US Foreign Policy and Internet*, Palgrave MacMillan, London.
• Morozov, E. (2009), "Cyber-Scare: The Exaggerated Fears over Digital Warfare", Boston Review, July/August 2009. http://bostonreview.net/archives/BR34.4/morozov.php
• Müller, V. C. (2016), Risks of Artificial Intelligence, CRC Press, Boca Raton.
• Ozeren, S. et al. (2007), *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, IOS Press, Amsterdam
• Rid, T. (2013), *Cyber War will not take place*, Oxford University Press, Oxford.
• Weimann, G. (2015), *Terrorism in Cyberspace. The Next Generation*, Columbia Univ. Press, New York.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies