COMMENTARY
OTTOBRE 2017

UE E CYBERSECURITY: UN NUOVO APPROCCIO STRATEGICO

LUIGI MARTINO

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

UE E CYBERSECURITY: UN NUOVO APPROCCIO STRATEGICO

Luigi Martino

UNIVERSITÀ DEGLI STUDI FIRENZE

Commentary

Ottobre 2017

RIGUARDO ALL'AUTORE

Luigi Martino si è laureato cum Laude in Relazioni Internazionali e Studi Europei presso la Facoltà di Scienze Politiche "Cesare Alfieri" di Firenze, con una Tesi sulla rilevanza strategica del cyberspace e i rischi di guerra cibernetica. si interessa, oltre che di Studi Strategici e Politica Internazionale, anche di Intelligence e Processi Decisionali. Attualmente, sempre alla "Cesare Alfieri", è Cultore della Materia in ICT Policies e insegna Cyber Security and International Relations. E' Phd Candidate alla Scuola Superiore Sant'Anna di Pisa, con un progetto di tesi sul miglioramento della Cyber Security per la protezione delle infrastrutture critiche dagli attacchi cyber, ed è consultant in Cyber Security del gruppo BV-Tech S.p.A. Dal 2016 è project manager del progetto di ricerca OSCE: "Enhancing the Implementation of Conflict Stemming From the Use of ICT's." un progetto di ricerca congiunto tra OSCE e Università di Firenze. È membro del Research Advisory Group of the Global Commission on the Stability of Cyberspace e del gruppo di esperti ENISA per l'implementazione della Direttiva Europea NIS. Dal 2017 e' membro del gruppo di lavoro Ise-shima G7 Cyber Group e del Forum for Cyber Expertise, dove rappresenta il Center for Cyber Security and International Relations Studies. Autore di numerose pubblicazioni in italiano, inglese e spagnolo su temi legati alla cyber security, cyber warfare, cyber intelligence e cyber diplomacy, ha curato, con Umberto Gori, il libro Intelligence e Interesse Nazionale, Aracne Editrice 2015.

UE E CYBERSECURITY: UN NUOVO APPROCCIO STRATEGICO[1]

La sicurezza dello spazio cibernetico è una catena resistente quanto il suo anello più debole. Occorre dunque mettere in campo un approccio olistico, perché iniziative parziali e non coerenti con una strategia di sistema rischiano di risultare il *weakest link* che indebolisce l'intera architettura. La Ue si è posta da tempo l'obiettivo di proteggere il mercato unico da potenziali esternalità negative rappresentate dalle minacce cibernetiche, ma è divenuta vieppiù evidente la necessità di dotare l'Ue di una strategia complessiva. La prima Strategia Ue in questo ambito, adottata nel 2013, ha segnato un punto di svolta, ma gli attacchi sempre più dannosi e le crisi internazionali scaturite da eventi occorsi nello spazio cibernetico hanno imposto un nuovo slancio. Lo dimostrano i documenti pubblicati il mese scorso dall'Ue, i quali, attraverso un'analisi dettagliata dei punti di forza e debolezza della EU Cyber Security Strategy 2013[2] contribuiscono a delineare la nuova linea di azione politica dell'Unione nel campo della cyber security. In particolare, il report Assessment of the EU 2013 Cyber Security Strategy[3] ha evidenziato la necessità di spostare il baricentro di azione dell'Ue da un pivot puramente economico-centrico (concentrato sul vecchio concetto open, safe and secure cyberspace) verso un approccio proattivo basato soprattutto su capacità di difesa, resilienza e deterrenza degli Stati membri e dell'Unione stessa.

La nuova Strategia, pur senza disconoscere la validità di quanto sinora fatto, tende dunque a basare la propria dottrina su tre assi fondamentali: la resilienza (intesa sia come la capacità degli Stati membri e dell'Ue nel suo complesso di dotarsi di infrastrutture informatiche o interdipendenti dai sistemi informatici più solide ed efficaci, sia come la capacità di produrre tecnologie sicure da immettere nel mercato europeo), la deterrenza (ossia la capacità politico-diplomatica e militare di dissuadere i potenziali avversari, statali e non, dal lanciare un attacco nei confronti degli Stati membri Ue e quella operativa di anticipare e/o reagire agli attacchi subiti) e, infine, la

[1] Apparso originariamente su https://www.ispionline.it/it/pubblicazione/ue-e-cybersecurity-un-nuovo-approccio-strategico-18224
[2] https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en
[3] https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF

cooperazione internazionale in ambito cyber (che ha il principale obiettivo di facilitare la cooperazione con i principali stakeholders dello spazio cibernetico, siano essi privati, Stati esterni all'Unione o Organizzazioni internazionali, in primis Onu, Osce e Nato, al fine di mitigare i rischi di *misunderstanding* ed *escalation*).

La resilienza è, secondo l'Ue, la condizione indispensabile per garantire una cyber security efficace ed efficiente. Dal 2004 l'organo deputato a questo obiettivo nel settore ICT europeo è l'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (Enisa), competente per il dialogo tra i Computer Emergency Response Teams nazionali, lo scambio di *best practices*, l'*early warning* su minacce specifiche. Il suo campo di azione, tuttavia, è limitato da un mandato temporaneo che non permette all'Agenzia di agire in chiave strutturata e strategica. E' per questo motivo che la Commissione ha proposto di modificare il mandato dell'Enisa da temporaneo a permanente, al fine di garantire una maggiore incidenza dell'Agenzia sia sul fronte interno dell'Unione (nel rapporto orizzontale e verticale tra Bruxelles e gli Stati membri) sia sul fronte esterno (attraverso il coordinamento e il dialogo con i Cert dei Paesi partner). Inoltre, l'idea di riformare l'Enisa è giustificata sia dalla necessità di innalzare il livello di resilienza dell'Unione Europea rispetto alle minacce cyber (comprese le minacce ai valori democratici dell'Ue) sia dall'esigenza di implementare ed attuare le policies approvate dall'Unione che avranno dirette ricadute sugli Stati membri, come la direttiva sulla sicurezza delle reti e dei sistemi informativi (c.d. direttiva Nis) e il nuovo regolamento sulla protezione dei dati personali (c.d. regolamento Gdpr). Infine, l'Enisa "riformata" non si limiterà a ricoprire un ruolo meramente consultivo ma, attraverso un ambizioso *action plan*, tenderà a sviluppare delle azioni preposte al fine di garantire un ambiente cyber sicuro e resiliente. In questo piano di azione si prevede ad esempio il rafforzamento delle tecniche di *info-sharing* tra il Cert-Ue, l'Europol e l'Intcen (centro di analisi di intelligence dell'Ue) e i vari Cert nazionali degli Stati membri al fine di creare una capacità fattuale di early warning degli incidenti e degli attacchi cyber.

Tuttavia l'azione dell'Ue, da un punto di vista tecnico ed operativo, non si limita al solo aspetto "security", ma tende anche ad intravedere le potenzialità e le opportunità offerte dall'arena digitale anche da un punto di vista economico. Non a caso, un aspetto fondamentale che riguarderà i prossimi obiettivi strategici dell'Unione Europea sarà lo sviluppo del mercato unico della cyber security, inteso soprattutto come

l'incremento di produzione e fornitura di prodotti, servizi e processi direttamente collegati all'economia digitale. A tal fine, la Commissione sta avviando una specifica consultazione sulla possibilità di creare un quadro europeo di certificazione di tutti i prodotti (hardware e software) e servizi utilizzati per gestire i sistemi ICT delle infrastrutture critiche a livello europeo. In questo modo, attraverso un approccio di "sicurezza fin dalla produzione" (security by design) si tenderà a creare un circolo virtuoso basato sugli investimenti in ricerca e sviluppo per prodotti e servizi "certificati" i quali, in ultima analisi, avranno una ricaduta positiva sull'innalzamento del livello di sicurezza informatica dell'UE.

Un altro aspetto fondamentale rientrante nel "piano di azione" dell'Ue è costituito dalla consapevolezza che un'efficace gestione degli incidenti informatici deve, essenzialmente, basarsi sul concetto di "rapidità" della risposta alle emergenze. La Commissione ha dunque avanzato la proposta di valutare la creazione di una clausola di solidarietà rivolta esplicitamente agli incidenti cibernetici, con un relativo fondo di risposta alle emergenze per affrontare i danni subiti dagli Stati membri a seguito di attacchi in questa dimensione.

Tuttavia, il punto cardinale dell'azione "operativa" svolta dall'Ue nel settore cyber rimane sempre l'obiettivo strategico di giungere a un innalzamento della consapevolezza dei cittadini e dei policy maker sulle minacce provenienti dal dominio cyber. È per questo che uno degli aspetti fondamentali che la Commissione intende perseguire è l'avvio di campagne di sensibilizzazione sulla minaccia cibernetica e la necessità di potenziare, tra operatori economici e semplici utenti, la cosiddetta igiene cibernetica (cyber hygiene), così evitare tutta quella messe di incidenti che si potrebbero evitare con il semplice buon senso (ricordiamoci che il malware WannaCry, che tanto ha spaventato nei mesi scorsi, sarebbe stato del tutto innocuo se gli utenti avessero gratuitamente aggiornato i loro sistemi). Altrettanta attenzione la Commissione ha dedicato al tema delle fake news, le quali costituiscono un serio pericolo per la stabilità dei paesi dell'Unione. Anche in questo caso, uno specifico ruolo è assegnato alla nuova Enisa.

Secondo il Joint Communication to the European Parliament and the Council "*resilience, deterrence and defence, building strong cybersecurity for the EU*", le capacità operative saranno un aspetto dirimente per la capacità della Ue nel suo complesso di fronteggiare la minaccia cibernetica. In questo senso, la nuova cyber strategy dell'Ue promuove un approccio proattivo per la gestione degli attacchi cibernetici. Gli

strumenti individuati dalla Comunicazione congiunta sono essenzialmente quattro: la deterrenza, la difesa attraverso un partenariato pubblico-privato, la diplomazia in campo cyber e la cooperazione esterna con partner ed altre organizzazioni.

Per quanto concerne la creazione di una deterrenza cibernetica efficace nell'Ue, il presupposto fondamentale sarà costituito dalla capacità dell'Ue di dotarsi di una serie di misure capaci di risolvere l'annosa questione dell'attribuzione degli attacchi, cercando quindi di creare una capacità fattuale di "tracciabilità" delle azioni commesse nel dominio cyber. In questo settore, gli organismi tecnico-operativi ricopriranno un ruolo fondamentale, in particolare attraverso lo scambio informativo tra gli stati membri e le agenzie dell'Ue, soprattutto al fine di garantire delle indagini veloci e delle risposte coordinate ed immediate.

La deterrenza sarà tanto più efficace, quanto più credibile sarà la capacità dell'Ue di dotarsi di sistemi di difesa capaci di contrastare e dissuadere gli attacchi informatici. Attualmente, l'Unione Europea ha concentrato la propria azione di difesa sul concetto classico di "security", valorizzando gli aspetti tecnici e "interni". Tuttavia, come sottolinea il Comunicato congiunto, al fine di garantire una migliore capacità di difesa e deterrenza, l'Unione Europea dovrà scindere gli aspetti "civili" del cybercrime (affrontandoli con un efficace partenariato pubblico-privato e con i classici strumenti della pubblica sicurezza di responsabilità primaria degli Stati membri, supportati dallo European Cybercrime Center - Ec3) dagli aspetti militari, al fine di avviare, in seno ai propri organismi politici, un approfondito dibattito sullo sviluppo di capacità militari di cyber defence.

Ulteriore elemento fondamentale della nuova cyber strategy è poi l'ideazione di un quadro per una risposta diplomatica comune dell'Ue nei confronti delle azioni ostili commesse tramite gli strumenti cyber. Attraverso questo quadro l'Ue mira a strutturare un'azione di prevenzione dei conflitti e a mitigazione delle minacce cibernetiche nel breve, medio e lungo periodo, al fine di influenzare il comportamento di eventuali attori aggressivi e contribuire ad una maggiore stabilità delle relazioni internazionali. A tal fine, la risposta diplomatica europea avrà pieno accesso a tutti gli strumenti previsti dalla Common Foreign and Security Policy, incluse, se necessario, misure restrittive e sanzioni.

Infine, l'Unione Europea si impegna a portare avanti in un'ottica di miglioramento le relazioni con i suoi paesi partner, la cooperazione Ue-Nato e il dialogo con le organizzazioni internazionali e regionali. Di particolare interesse, in questo settore, è la volontà dell'Unione Europea di adottare un piano di cooperazione allo sviluppo nel campo della cyber security attraverso programmi di capacity building indirizzati a quei Paesi extra UE che, a causa di inadeguati livelli di sicurezza informatica, possono rivelarsi fattori di rischio per la sicurezza dell'Unione e degli Stati membri. Allo stesso tempo, l'Ue riconosce le iniziative di cyber diplomacy e di trust building avviate anche da altri attori internazionali e regionali, come l'Onu e l'Osce, sottolineando come una più efficace diplomazia in questo settore debba basarsi non solo sulle iniziative bilaterali ma anche sui fori multilaterali, al fine di produrre degli strumenti utili per mitigare il rischio di escalation politico-militare dentro e fuori i confini dell'Ue.

Il percorso per rendere operative tutte queste innovazioni non sarà ovviamente privo di ostacoli, ma è ormai evidente che la Commissione può contare su di un livello di consapevolezza degli Stati membri ben maggiore che in passato, e sulla chiara percezione che, seppure con una stringente applicazione del principio di sussidiarietà, l'Unione Europea è un attore in grado di fornire un indubbio valore aggiunto nella protezione dello spazio cibernetico europeo.

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