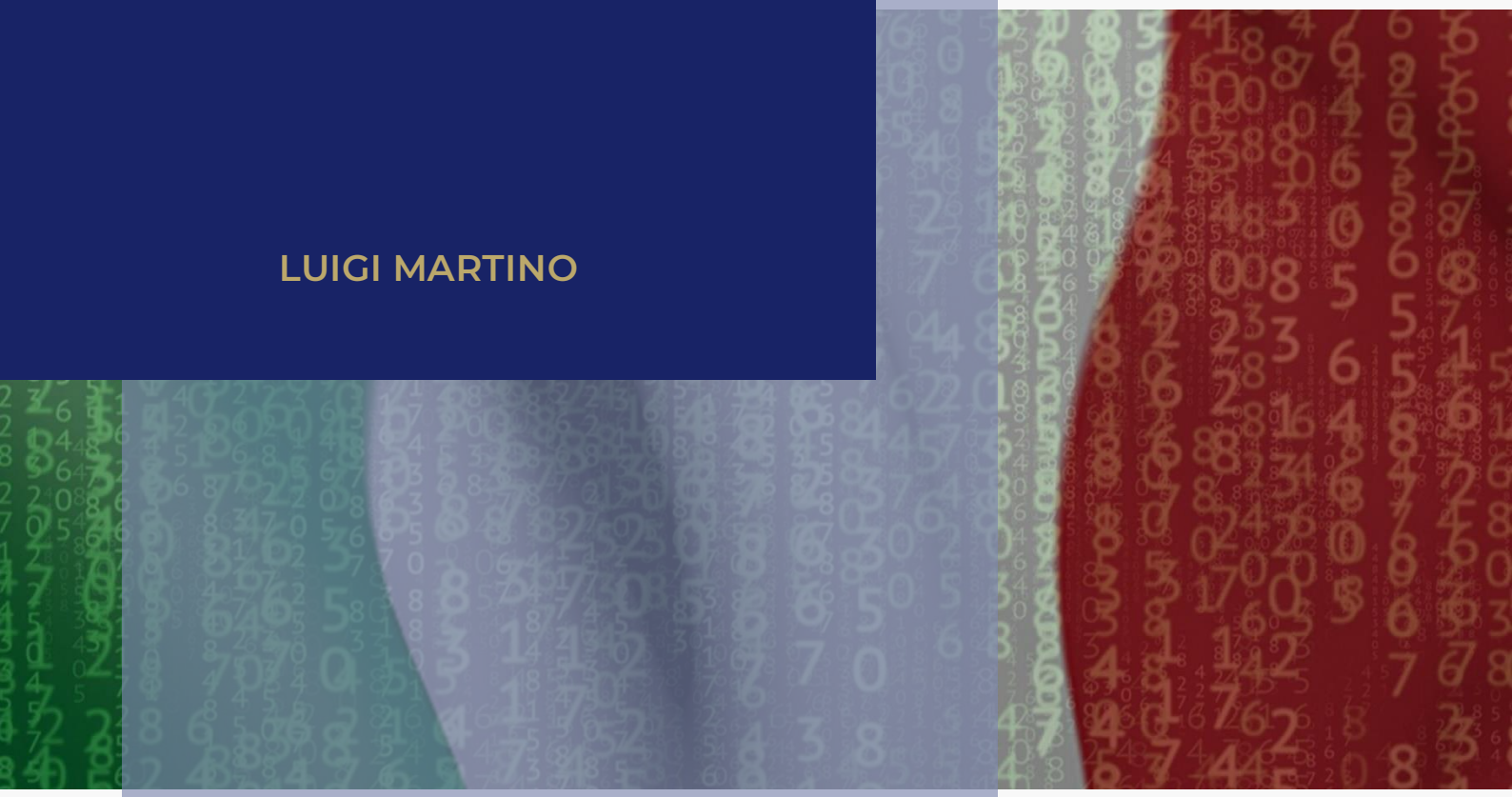
COMMENTARY
AGOSTO 2019

SPAZIO CIBERNETICO: LE MINACCE, I RISCHI E LE OPPORTUNITÀ PER L'ITALIA

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

SPAZIO CIBERNETICO:
LE MINACCE, I RISCHI E LE OPPORTUNITÀ PER L'ITALIA

Luigi Martino

UNIVERSITÀ DEGLI STUDI FIRENZE

Commentary

Agosto 2019

RIGUARDO ALL'AUTORE

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

SPAZIO CIBERNETICO: LE MINACCE, I RISCHI E LE OPPORTUNITÀ PER L'ITALIA[1]

Il Documento di Sicurezza Nazionale del 2018 – allegato alla relazione annuale che i Servizi di Intelligence italiani presentano al parlamento – rappresenta un'ottima fonte primaria dalla quale attingere per riuscire a comprendere **l'entità delle minacce cyber** in Italia. Nel documento infatti si sottolinea, in modo incontrovertibile, come la minaccia cyber rappresenti **un serio rischio per gli interessi economici, scientifici e militari** del nostro paese. Infatti, dall'analisi dei dati contenuti nel Documento affiora chiaramente che le azioni malevoli protratte dal cyberspazio hanno avuto un incremento esponenziale nell'ultimo anno. Infatti, il documento del 2018 recita:

Emerge un numero complessivo di azioni ostili più che quintuplicato rispetto al 2017, prevalentemente in danno dei sistemi informatici di pubbliche amministrazioni centrali e locali (72%). Un'analisi più approfondita degli eventi che hanno interessato i soggetti pubblici attesta un incremento pari a oltre sei volte (+561%) rispetto all'anno precedente. È stato rilevato, in particolare, un sensibile aumento di attacchi contro reti ministeriali (24% delle azioni ostili, in aumento di 306 punti percentuali) e contro infrastrutture IT riconducibili ad enti locali (39% del totale del periodo in esame, con una crescita in termini assoluti pari a circa 15 volte). [2]

L'allarme lanciato dai Servizi di Intelligence italiani evidenzia, allo stesso tempo, un ulteriore dato allarmante, ovvero che le minacce provenienti dal mondo cyber hanno raggiunto livelli di sofisticatezza tali per cui ad essere in pericolo non sono più "esclusivamente" i meno avvezzi ai rischi provenienti dal cyberspazio, ma **l'intero apparato della pubblica amministrazione** centrale e locale. [3]

Si evidenzia altresì come l'Italia sia sempre più a rischio di minacce "sistemiche", ovvero attività malevole condotte "per procura" ed

[1] Apparso originariamente su ISPI, https://www.ispionline.it/it/pubblicazione/spazio-cibernetico-le-minacce-i-rischi-e-le-opportunita-litalia-23774

[2] Cfr. Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, "Documento di Sicurezza Nazionale", in *Relazione sulla politica dell'informazione per la sicurezza 2018.*

[3] *Ibidem*

effettuate da attori non statali i quali, attraverso attacchi informatici mirati contro attori pubblici (pubblica amministrazione o funzionari pubblici) e attori privati (che gestiscono o possiedono infrastrutture critiche) prediligono target strategici, attraverso soprattutto **l'esfiltrazione di informazioni** sensibili e riservate.[4]

Alla luce di quanto detto sopra, le priorità relative alla protezione della competitività, della sicurezza nazionale e della stessa sovranità statale assumono quindi **elevata rilevanza strategica** (e quindi politica), visto che la minaccia di tipo cibernetico ha assunto contorni sofisticati, così come sempre più spesso le azioni cyber vengono strumentalizzate a fini di competizioni *intra* e *inter* nazionale.

Nello specifico, le sfide provenienti dal mondo cyber hanno **caratteristiche eterogenee**, di provenienza esogena ed endogena. Per quanto concerne le prime è del tutto evidente che, come si evince da recenti riscontri, nella "quinta dimensione della conflittualità"[5] siano sempre più labili i confini tra amico e nemico, alleato e avversario.

L'Italia, in questo senso, si trova a dover fronteggiare una crescente perniciosità delle azioni cyber le quali, grazie alla *plausible deniability*, riescono a garantire un elevato livello di anonimato con **relativa immunità** rispetto all'attribuzione della responsabilità. Non a caso da varie ricerche è emerso come vi sia un interesse sempre maggiore nei confronti del *know-how* italiano, il quale viene minacciato da **crescenti campagne di spionaggio** informatico dedito anche alla sottrazione di segreti industriali e brevetti innovativi.

La crescita poi delle minacce esogene che interessano l'Italia va messa in correlazione con lo sviluppo innovativo e tecnologico che pone sfide di natura "sistemica", ovvero relative alla capacità di sviluppare competenze di difesa di un perimetro che di fronte alla diffusione dell'intelligenza artificiale, del 5G e dell'*Internet of Things* (IoT), diventa sempre più ampio, **interconnesso e interdipendente**. Basti pensare alla sfida relativa al 5G (sfida non solo politico-commerciale ma anche tecnica), nella quale possono emergere problemi rispetto al Regolamento Europeo per la Protezione dei Dati (GDPR), qualora tali dati venissero gestiti da infrastrutture che fanno capo a paesi terzi, i

[4] *Ibidem*
[5] Luigi Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in Politica & Società, Fascicolo 1, gennaio-aprile 2018.

quali non hanno nessun obbligo nei confronti del menzionato regolamento. E ancora la minaccia relativa al 5G rispetto alla **sempre maggiore labilità esistente tra settore civile e militare** e quindi rispetto alle capacità di difendere il perimetro vitale della riservatezza delle informazioni.

In quest'ottica si inseriscono le sfide endogene, fra cui la questione "culturale" della cyber security che, ancora oggi, stenta ad affermarsi in Italia. Come già sottolineato, l'Italia dovrebbe affrontare i rischi cyber attraverso un'elevata capacità di governare le minacce tramutandole in **opportunità per incrementare la propria competitività** sul piano internazionale. [6]

Tuttavia, la bassa diffusione della cultura della cyber security in Italia mette in serio pericolo la tenuta del sistema paese.

Lo dimostrano i dati del Rapporto Clusit, i quali mettono in evidenza come gli attacchi cyber (soprattutto di tipo criminale) abbiano subito un salto "quantico" e un *trade-off* negativo **fra azioni criminali e consapevolezza degli utenti**.[7]

Un'altra sfida endogena per l'Italia è rappresentata dalla capacità dei decisori politici e istituzionali di tramutare la cyber security **da minaccia a opportunità** economica, culturale e industriale per il sistema paese.

Nel tentativo di fronteggiare le minacce esogene ed endogene, l'Italia ha messo in pratica le indicazioni contenute nel Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e gli obiettivi operativi previsti dal "Piano Nazionale", avviando così **una serie di azioni concrete** sui rischi provenienti dall'arena digitale con il prezioso contributo del comparto intelligence e, in particolare, del Nucleo per la Sicurezza Cibernetica (coordinato dal Vice Direttore del DIS con delega alla cyber security). Tra le azioni, vi sono:

- La realizzazione di un "perimetro di sicurezza nazionale cibernetica", volto ad elevare i livelli di sicurezza degli assetti vitali del paese;
- La costituzione di un ulteriore gruppo di lavoro, volto ad individuare linee guida per un procurement "sicuro" di prodotti e servizi ICT per la PA, coordinato dall'Agenzia per l'Italia Digitale

[6] Cfr. Luca Zorloni, *Sicurezza informatica, la strategia dell'Italia contro gli attacchi hacker*, in Wired
[7] Cfr, Associazione Italiana per la Sicurezza Informatica, *Rapporto Clusit 2019*.

(AgID), al quale hanno aderito, oltre ai componenti NSC, anche Consip;

- L'avvio di una collaborazione con il MiSE per la creazione – in conformità alle normative italiane ed europee – del Centro di Valutazione e Certificazione Nazionale (CVCN) per la verifica delle condizioni di sicurezza delle soluzioni ICT destinate al funzionamento di reti, servizi delle infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale[8].

Affinché queste azioni di contrasto dei rischi e mitigazione delle minacce possano realizzarsi è necessario, oltre alla creazione di un quadro di politiche create *ad hoc*, anche la capacità di comprendere che, rispetto alle minacce provenienti dal cyberspazio, deve vigere una situazione "win-win" **tra enti pubblici, aziende e società civile** laddove tutti gli attori in campo ricevano il beneficio dalla collaborazione sotto forma di partnership attraverso un approccio di sicurezza partecipata.

[8] Cfr. Presidenza del Consiglio dei Ministri, op. cit.

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