L'impatto sulla sicurezza nazionale della digitalizzazione forzata da COVID-19. Possibili strategie di contrasto alla minaccia cyber

Federico Bertola

Un processo di digitalizzazione che si sarebbe verificato in anni o decenni, con l'emergenza COVID-19 si è verificato in giorni e in mesi. Ciò ha inevitabilmente portato a ricadute e impatti sulla sicurezza nazionale: un aumento esponenziale degli episodi di attacchi provenienti dal dominio cibernetico, insieme ad una parallela cyberpandemia *di attacchi alle infrastrutture sanitarie, a disinformazione e rabbia sociale sui* social media*, sono solo alcuni degli effetti. La libertà dei cittadini e l'integrità della Repubblica risultano essere dunque sempre più connesse alla sicurezza delle reti. Di fronte a questa recrudescenza della minaccia cyber, si rileva necessaria una risposta di sistema fondata sulla "collaborazione": tra istituzioni nazionali, tra pubblico e privato e a livello internazionale. Di fronte a questa evoluzione della minaccia, infatti, il Sistema Paese non può che rispondere in modo organico e coordinato a livello nazionale e internazionale.*

L'emergenza COVID-19 ha fatto tornare in primo piano nell'agenda dei governi i temi della sicurezza nazionale, del ruolo dell'intelligence e della cybersecurity. La sicurezza nazionale non comprende al suo interno solamente le minacce di lunga tradizione, come il terrorismo, la criminalità organizzata, la difesa degli asset militari e strategici del Paese; essa si prefigge di tutelare la Nazione anche da minacce multiformi ed articolate come quelle provenienti dal mondo economico-finanziario, o di natura cibernetica o sanitaria, e tutte le minacce che vanno a toccare gli interessi più rilevanti e irrinunciabili dello Stato[1]. In un mondo interconnesso come quello attuale, l'azione di protezione della sicurezza nazionale risulta inoltre caratterizzata dalla interdipendenza dei diversi aspetti sopra citati.

[1] Marco Valentini, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*. Il grifone. Napoli, Editoriale scientifica, 2017.

La crisi provocata dalla pandemia ha portato quello che era un fenomeno di graduale digitalizzazione dei processi ad un'accelerazione improvvisa e ad un allargamento delle attività erogate attraverso mezzi informatici: non solo il lavoro, ma anche le chiamate tra privati, le relazioni interpersonali tra amici e parenti, la didattica a distanza, gli acquisti. Il Ministero del Lavoro ha rilevato come a fine aprile 2020 il numero di lavoratori italiani attivi in modalità smart working fossero circa 2 milioni, a fronte dei circa 200mila lavoratori da remoto prima dell'avvento dell'emergenza sanitaria[2]. Eventuali interruzioni di servizio possono così avere sempre più impatto sull'economia e l'integrità del Paese, poiché la superficie di possibili attacchi informatici è aumentata esponenzialmente senza preparazione e pianificazione adeguate. L'aggressione cibernetica sistematica, anche qualora non attacchi infrastrutture critiche ma punti per mero lucro criminale ad imprese e famiglie, "investe l'intero Sistema Paese, assurgendo al grado di minaccia alla sicurezza nazionale"[3].

La Polizia Postale ha registrato nei primi dieci mesi del 2020 un incremento del 353% degli attacchi rilevati e del 436% di segnalazioni di *fake news*: la minaccia cyber si è dunque evoluta, portando a scenari nuovi e richiedendo risposte altrettanto innovative[4]. La natura globale dell'emergenza e le ricadute asimmetriche degli effetti hanno fatto comprendere la necessità di un approccio olistico alle minacce ibride.

Tra gli impatti sulla sicurezza nazionale del massiccio ricorso agli strumenti digitali imposto dalla pandemia, è da riscontrare in primo luogo una parallela cd. "cyber-pandemia"[5]: nel 2020, infatti, si è registrato il picco più alto di attacchi contro il sistema sanitario, a livello nazionale ma anche internazionale. In particolare, si è

[2] Ministero del Lavoro e delle Politiche Sociali. 2020. "Sono Più Di 1 Milione E 800 Mila I Lavoratori Attivi In Modalità Smart Working". https://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/Sono-piu-di-1-milione-800-mila-i-lavoratori-attivi-in-modalita-smart-working.aspx.

[3] "Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico.", § IV Commissione della Camera dei Deputati, 2017.

[4] Ministero dell'Interno, "Report 2020 della Polizia Postale: in aumento le minacce e le truffe sul web", gennaio 2021.

[5] Aldo Di Mattia, a c. di, "La prima CyberPandemia nella storia dell'umanità", *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia. Edizione ottobre 2020*, ottobre 2020, 85–88.

rilevato un eccezionale incremento di *ransomware* contro gli ospedali, con un aumento registrato nel marzo 2020 di oltre il 70% a livello globale e perdurato poi per tutto l'anno: tra essi il primo ad aver causato la morte di una persona si è verificato all'ospedale di Düsseldorf [6]. Di particolare rilevanza anche il tentativo di attacco alle strutture dell'ospedale Lazzaro Spallanzani di Roma che ha provocato allerta ed immediata vigilanza da parte degli apparati di sicurezza. In particolare, è stato riunito il Nucleo Sicurezza Cibernetica, atto ad assicurare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale, alla presenza delle agenzie di intelligence e della Polizia Postale[7]. Dalla risposta a tale attacco emerge chiaramente la necessaria e costante collaborazione tra apparati di intelligence e Forze di Polizia nella protezione del Sistema Paese dalle minacce cibernetiche. Nello specifico, per quanto riguarda il settore sanitario, particolare rilevanza per i profili di sicurezza nazionale rappresentano gli attacchi perpetrati nei confronti della filiera dei vaccini, tra i cui bersagli sono figurati la European Medicine Agency (EMA) e diverse aziende anche nazionali coinvolte in prima linea nella filiera vaccinale[89].

Altro attacco di rilevanza strategica, avvenuto nel periodo dell'emergenza pandemica, ha riguardato la piattaforma *SolarWinds Orion* per cui, a partire da marzo, alcuni hacker si sono introdotti all'interno delle reti e dei sistemi informatici di enti governativi e privati in tutto il mondo spiando le loro mosse e in alcuni casi trafugando dati

---

[6] Filip Truță, a c. di, "Sicurezza nel settore sanitario – Perché gli ospedali sono così violabili?", *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia. Edizione ottobre 2020*, ottobre 2020, 193–97.

[7] Sistema di informazione per la sicurezza della Repubblica, "Riunione straordinaria del Nucleo Sicurezza Cibernetica: tentativo di attacco a Spallanzani, allertata rete sanitaria nazionale. Altissima vigilanza da parte degli apparati di sicurezza", sicurezzanazionale.gov, aprile 2020.

[8] European Medicines Agency, "Cyberattack on EMA - Update 6", European Medicines Agency, 22 gennaio 2021, https://www.ema.europa.eu/en/news/cyberattack-ema-update-6.

[9] "Vaccini: attacchi hacker alla Irbm, i Pm di Roma avviano un'indagine - Lazio", *Agenzia ANSA*, 30 dicembre 2020, par. Lazio, https://www.ansa.it/lazio/notizie/2020/12/30/vaccini-attacchi-hacker-alla-irbm-i-pm-di-roma-avviano-uni ndagine-_8f45482c-3b5d-4dd5-b1dc-8aa99e0e3b06.html.

particolarmente sensibili[10]. La risposta immediata è stata dell'intelligence e, in particolare, è risultato decisivo nel far fronte a tale attacco globale il continuo contatto con la rete di collegamento europeo "CyCLONe", che si propone di agevolare la cooperazione tra le autorità nazionali di cybersecurity in caso di incidenti informatici destabilizzanti[11]. Questa offensiva e la relativa risposta hanno evidenziato che gli attacchi informatici non sono limitati entro confini geografici, e possono colpire contemporaneamente diversi attori globali; pertanto, sarebbe necessaria la collaborazione tra i diversi Stati e tra organizzazioni pubbliche e private per concertare una reazione efficace.

Un ruolo di primo piano nell'impatto di questa digitalizzazione forzata sulla sicurezza nazionale è giocato inoltre dai *social media*[12]. Questi ultimi hanno conosciuto nel periodo pandemico una crescita esponenziale nel volume e tempo di utilizzo, diventando un terreno multipolare e soggetto a campagne di disinformazione, oltre che teatro di una polarizzazione delle opinioni[13]. Come emerso nell'autunno 2020 in Italia, con alcune proteste nelle principali piazze del Paese, e in particolare a Napoli, Milano, Roma, Firenze e Bologna, la popolazione, talvolta incitata da organizzazioni criminali, si è organizzata tramite gruppi *social* provocando poi scontri e problemi di ordine pubblico[14]. A livello internazionale, emblematico è il caso dell'attacco al Campidoglio degli Stati Uniti, dove l'organizzazione e la radicalizzazione dei soggetti attaccanti è

[10] Sistema di informazione per la sicurezza della repubblica, "Hackeraggio della piattaforma Solarwinds: Riunito il nucleo per la sicurezza cibernetica.", sicurezzanazionale.gov, dicembre 2020.

[11] Sistema di informazione per la sicurezza della repubblica, "Hackeraggio della piattaforma Solarwinds: Riunito il nucleo per la sicurezza cibernetica.".

[12] Emilio Ferrara, Stefano Cresci, e Luca Luceri, "Misinformation, manipulation, and abuse on social media in the era of COVID-19", *Journal of Computational Social Science* 3, n. 2 (1 novembre 2020): 271–77, https://doi.org/10.1007/s42001-020-00094-5.

[13] Ferrara, Cresci, e Luceri, "Misinformation, manipulation, and abuse on social media in the era of COVID-19".

[14] Annalisa Camilli, "Da dove viene la rabbia di chi protesta a Napoli", *Internazionale*, 2 novembre 2020, https://www.internazionale.it/reportage/annalisa-camilli/2020/11/02/napoli-proteste-lockdown.

avvenuta tramite gruppi chiusi all'interno dei *social media*[15]. Con questi fatti si è definitivamente ribaltata l'idea che quanto accade nel mondo virtuale non abbia poi un impatto sul mondo reale. In seguito a tali eventi, inoltre, alcune delle *Big tech*[16] hanno proceduto ad eliminare diversi profili ritenuti pericolosi, oltre che a sospendere alcune piattaforme *social*[17]: tali azioni hanno posto in primo piano il tema del bilanciamento tra la libertà di espressione e i poteri di aziende private[18]. Nel periodo post-COVID-19 è quindi possibile ipotizzare come la rabbia sociale - generata da difficoltà economiche crescenti e contestualmente fomentata all'interno di gruppi *social* - possa sfociare in possibili rimostranze e rappresaglie nei confronti delle Istituzioni. Il che rappresenta una possibile minaccia alla sicurezza nazionale, all'ordine pubblico e all'integrità delle istituzioni repubblicane.

Con l'emergenza sanitaria, dunque, è emerso in modo ancora più evidente come l'integrità e la prosperità del Paese sia sempre più dipendente dalla protezione dello spazio cibernetico. Risulta allora impellente garantire nel cyberspazio il rispetto dei diritti e dei doveri già consolidati nella società civile e nella comunità nazionale ed internazionale.

A livello normativo, su questo fronte, è da segnalare il progressivo rafforzamento dell'architettura nazionale cyber dal 2018, in seguito all'attuazione della direttiva NIS con il D.Lgs. n. 65/2018 e la previsione nel "perimetro di sicurezza nazionale

---

[15] Sheera Frenkel, "The Storming of Capitol Hill Was Organized on Social Media", *The New York Times*, 6 gennaio 2021, par. U.S., https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.

[16] Per *Big tech* si intendano le cinque più grandi aziende tecnologiche statunitensi - Alphabet (Google), Amazon, Apple, Facebook e Microsoft.

[17] 'How Big tech companies responded to the storming of the Capitol', *The New York Times*, 11 gennaio 2021 https://www.nytimes.com/2021/01/11/business/how-big-tech-companies-responded-to-the-storming-of-the-capitol.html.

[18] Vivek Ramaswamy and Jed Rubenfeld, "Save the Constitution From Big Tech. Congressional Threats and Inducements Make Twitter and Facebook Censorship a Free-Speech Violation.", *Wall Street Journal*, 11 gennaio 2021, par. Opinion, https://www.wsj.com/articles/save-the-constitution-from-big-tech-11610387105.

cibernetica"[19] di procedure di raccordo e coordinamento tra Autorità competenti e soggetti inclusi. Pertanto, alla base del contrasto della minaccia cyber, le principali forme di strategie di Sistema consistono nella collaborazione tra i diversi attori coinvolti, a tutti i livelli.

Il primo pilastro alla base del contrasto alla crescente minaccia cibernetica consta nella collaborazione tra le diverse istituzioni coinvolte a livello nazionale. In particolare, è da sottolineare la collaborazione necessaria tra apparati di *law enforcement*, intelligence e Difesa, nel rispetto degli ambiti di competenza determinati dalla legge per ciascun attore, garantendo così il fine ultimo della sicurezza della Repubblica.

In secondo luogo, vista e considerata la de-territorialità della minaccia cibernetica, i confini nazionali non rappresentano più un sufficiente perimetro operativo né uno strumento utile al contenimento e alla prevenzione della minaccia stessa. Lo dimostrano, ad esempio, le operazioni congiunte a livello comunitario, come l'operazione antiterrorismo online *Referral Action day*[20] condotta da Europol insieme alle diverse forze di polizia internazionali nel luglio 2020, oltre che la risposta all'attacco SolarWinds attraverso la rete di collegamento europeo CyCLONe. Al fine di contenere i pericoli provenienti dal quinto dominio è necessaria, dunque, una collaborazione tra le diverse Forze di Polizia, d'Intelligence e di Difesa anche a livello internazionale, insieme ad un'uniformità dei parametri normativi, che rendano agevole il coordinamento nella risposta.

A ciò è fondamentale aggiungere che l'interdipendenza delle reti, unita all'asimmetricità e pervasività della minaccia, rendono necessario assicurare un accettabile livello di sicurezza *cyber* da parte del Sistema Paese, attraverso un approccio olistico che vada a perseguire l'obiettivo di raggiungere quella collaborazione tra pubblico e privato in grado di assicurare un sistema di risposta solido e coeso. Con

[19] Legge 18 novembre 2019, n. 133 recante "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica".

[20] "Rimossi dal web manuali e altri contenuti incitanti al terrorismo", Ministero dell'Interno, luglio 2020, https://www.interno.gov.it/it/notizie/rimossi-dal-web-manuali-e-altri-contenuti-incitanti-terrorismo.

strumenti e processi di circolazione informativa, di collaborazione nella risposta agli incidenti gravi, di scambio e di sviluppo delle *best practice*, è possibile sviluppare sinergie virtuose tra università, imprese e sistema dei pubblici poteri, in grado di mettere a fattor comune le attuali capacità tecnologiche, industriali e di ricerca a livello nazionale. Tale collaborazione deve anche, d'altro canto, agevolare la tutela da parte dello Stato della sovranità rispetto ad attori privati che ne minano la credibilità e l'autorità in modo sempre più pervasivo: lo spazio digitale, infatti, non può e non deve rappresentare un luogo al di fuori della legge, e le istituzioni democratiche devono essere in grado di garantire spazi digitali sicuri, aperti ed affidabili, attraverso la chiara definizione di una strategia di *governance* dello spazio digitale da attuare tramite puntuali interventi regolatori, senza lasciare che siano solo le aziende private a stabilirne le regole

La digitalizzazione forzata ha avuto dunque impatto sulla sicurezza nazionale, rendendo in particolare evidente come la libertà e la stabilità del Paese siano intimamente connesse alla sicurezza delle reti. Risulta pertanto fondamentale attuare un sistema nazionale resiliente ed efficace nei confronti delle nuove tecnologie, reso solido dalla collaborazione tra istituzioni, tra pubblico e privato e a livello internazionale. Solamente attraverso una risposta olistica di sistema, dunque, si potrà rispondere efficacemente alla crescente minaccia cyber.

FEDERICO BERTOLA è Analista nel Team Cyber, Terrorism and Domestic Extremism presso The Counterterrorism Group (CTG) di Washington DC. Ha conseguito la Laurea Magistrale in Politiche per la Sicurezza all'Università Cattolica di Milano, con una tesi sulla minaccia cyber alla sicurezza nazionale, e la Laurea Triennale in Scienze dei Servizi Giuridici all'Università degli Studi di Milano. Nel suo ruolo presso The Counterterrorism Group, si occupa di analisi strategica della minaccia cibernetica, di terrorismo e monitoraggio di movimenti eversivi. Autore di pubblicazioni, tra cui "Drug trafficking on Darkmarkets: How Cryptomarkets are Changing Drug Global Trade and the role of Organised Crime" (American Journal of Qualitative Research, 2020) e

articoli di analisi, tra cui “US Election 2020 Interference”, “Insider Threats and Espionage in Police Departments”, “Hard Lessons Learned: Analysis of Immediate Failures and Inconsistencies with U.S. Capitol Security” (The Counterterrorism Group, 2020).
