**La bio-insicurezza globale dopo la pandemia da SARS-CoV-2 e la necessità di una strategia nazionale di biodifesa**

Massimo Amorosi

*La pandemia da SARS-CoV-2 ha fatto emergere scenari globali di bio-insicurezza, imputabili al concorso di fattori naturali e antropici, quali la proliferazione dei laboratori di tipo BSL-3 e BSL-4, la digitalizzazione e democratizzazione delle scienze biologiche, il fenomeno della convergenza tecnologica e i rischi che promanano da talune partnership internazionali, nonché la crisi dei tradizionali regimi internazionali di controllo degli armamenti, in primis della Convenzione sulle Armi Biologiche. Tutti questi fattori considerati insieme confermano un'urgente necessità di consolidare gli strumenti di biosicurezza, ridurre i rischi biologici posti dai progressi tecnologici, creare nuovi approcci per migliorare la sorveglianza delle malattie infettive, nonché identificare e colmare i* gap *per rafforzare le capacità di sicurezza sanitaria globale. Nonostante le menzionate sfide, la biosicurezza rimane una priorità di sicurezza ancora troppo sottostimata e sottofinanziata in gran parte dei Paesi avanzati. L'Italia potrebbe essere la prima a dotarsi di un'organizzazione strategica di biodifesa rispetto ai rischi biologici emergenti, di cui il comparto della Difesa dovrebbe essere uno dei pilastri. La recente pandemia ha dimostrato che non vi è alcuna differenza nell'attivazione dei meccanismi di preparazione e risposta ad una minaccia biologica emergente, a prescindere dalla sua origine naturale, accidentale, o deliberata.*

---

### *L'evoluzione dei rischi biologici emergenti*

La pandemia da SARS-CoV-2 ha fatto emergere scenari di bio-insicurezza su scala globale, imputabili al concorso di fattori naturali e antropici, alla proliferazione dei laboratori del tipo BSL-3 e BSL-4[1], alla digitalizzazione e democratizzazione delle

[1] BSL (Biological Safety Level) indica il livello di bio-protezione del laboratorio. Il livello 3 corrisponde ad un livello elevato, mentre il successivo livello 4 equivale al livello massimo. I principali criteri utilizzati per assegnare un microrganismo ad un determinato livello BSL sono l'infettività, la gravità della patologia, la trasmissibilità, la natura del lavoro di laboratorio da compiere, e l'origine dell'agente patogeno. L'origine del patogeno può essere autoctona (rispetto al quale il nostro sistema immunitario è più predisposto) o esotica. Il livello BSL-4 riguarda manipolazioni a rischio molto elevato di organismi esotici che causano

scienze biologiche e, più in generale, dal fenomeno della convergenza tecnologica, dai rischi che promanano da talune partnership internazionali in ragione del trasferimento di tecnologie e *know-how* verso Paesi che non dispongono di adeguati protocolli di biosicurezza, nonché dalla crisi dei tradizionali regimi internazionali di controllo degli armamenti, in primo luogo della Convenzione sulle Armi Biologiche.

Globalmente, sono operativi o in fase di realizzazione più di cinquanta laboratori BSL-4, dispersi fra Asia, Africa, Europa, Russia e Stati Uniti, secondo un rapporto dell'Organizzazione Mondiale della Sanità del 2017[2]. La supervisione governativa appare fondamentale per la sicurezza di tali laboratori, anche se il fulcro resta costituito dal personale che vi opera, dilatando in tal modo il rischio dell'"insider threat". Data la controversia sulle cosiddette ricerche "gain-of-function"[3] e i potenziali incidenti che coinvolgono i laboratori[4], appare densa di rischi la competizione geopolitica in atto volta a realizzare in numeri crescenti tali strutture in cui si effettuano manipolazioni ad alto rischio di microrganismi, anche a fronte di batteri o virus nuovi, ossia con differenze genetiche rispetto ai microrganismi originari, oppure emergenti, cioè contro i quali non sono disponibili appositi farmaci e vaccini.

Nel contesto di una più accentuata competizione internazionale tra le grandi potenze, le crisi e le tensioni che originano dai cambiamenti climatici e dagli interventi distorsivi da parte dell'uomo sull'ambiente potrebbero creare un terreno fertile per l'insorgere di istanze radicali, che potrebbero sfociare anche nel ricorso ad agenti biologici. Un solo precedente può essere preso come riferimento e risale al 1972, quando

---

patologie gravi per le quali non esistono trattamenti. Amorosi, 2020, *Il patogeno come arma*, LiMeS Rivista Italiana di Geopolitica.

[2] World Health Organization, 2017, *WHO Consultative Meeting on High/Maximum Containment (Biosafety Level 4) Laboratories Networking*, International Agency for Research on Cancer (IARC), Lione.

[3] Tali ricerche sono state associate alla modificazione del genoma di un microrganismo allo scopo di conferirgli una funzione "nuova" o "potenziata" per fini di studio, quali ad esempio un'accresciuta virulenza per gli esseri umani oppure la capacità di eludere il sistema immunitario dell'ospite. Hanno risvolti positivi, ad esempio, per la comprensione della resistenza ai farmaci di taluni patogeni, ma non senza potenziali derive e rischi per la salute pubblica e la sicurezza. Patogeni a basso rischio possono essere modificati per diventare agenti a rischio elevato. Alcune caratteristiche dei microrganismi possono inoltre essere ottenute in laboratorio con tecniche di selezione su coltura, che non richiedono manipolazioni che lasciano tracce.

[4] Anche laboratori di bio-contenimento di livello 4, ritenuti sicuri per gli standard internazionali, non sono stati risparmiati da incidenti. Si pensi, ad esempio, al rilascio del virus dell'afta epizootica nel 2007 dai laboratori britannici di Pirbright. Amorosi, 2020, *Perché una nuova missione internazionale per accertare l'origine del Sars CoV-2*, Roma.

il gruppo anarchico ecologista RISE aveva tentato di diffondere almeno un agente patogeno nel sistema di distribuzione dell'acqua di Chicago.

Il 75% delle malattie emergenti sono di origine animale, mentre l'80% degli agenti patogeni classificabili per un potenziale uso bioterroristico sono zoonosi, ossia malattie trasmissibili dall'animale all'uomo. I sistemi contemporanei di sorveglianza di patogeni pericolosi per la salute pubblica rimangono però separati per esseri umani e animali. Si avverte pertanto la necessità di approfondire la comprensione dell'interfaccia o trasmissione di agenti patogeni tra l'ambiente, la fauna selvatica, gli animali e l'uomo come parte di un complesso sistema socio-ecologico. L'ultima emergenza pandemica ha confermato che occorre potenziare la sorveglianza integrata e la risposta alle malattie infettive emergenti, evidenziando la stretta correlazione tra questa e le necessarie misure di prevenzione e preparazione a tale tipologia di minacce.

A destare particolare preoccupazione sono le malattie trasmesse da vettori, molte delle quali sono zoonotiche[5] e considerate nell'Unione Europea malattie infettive emergenti, ossia che compaiono per la prima volta in una popolazione o che possono essere già esistite in passato, ma la cui incidenza o diffusione geografica è in rapido aumento. Altri fattori, tra cui le condizioni climatiche, possono influenzarne la diffusione e persistenza in nuove aree.

Il quadro che emerge dalle *lessons learned* dell'attuale pandemia da coronavirus è stato efficacemente sintetizzato dal Segretario Generale della NATO Stoltenberg, allorché ha sottolineato che "il nostro compito principale è, ovviamente, fornire deterrenza e difesa e assicurarci che questa crisi sanitaria non si trasformi in una crisi di sicurezza"[6].

Ciò è tanto più vero in quanto la partita tecnologica internazionale si sostanzierà in una sfida geopolitica senza precedenti: la crescente convergenza tra tecnologie emergenti e *disruptive*[7] innescherà dinamiche di iper-competizione con l'affacciarsi di nuovi rischi in termini di sicurezza, anche militare, con effetti in qualche modo simili a quelli

[5] Tra queste si annoverano, ad esempio, la malattia di Lyme, l'encefalite trasmessa da zecche, il virus del Nilo occidentale, la Leishmaniosi e la febbre emorragica Congo-Crimea.

[6] North Atlantic Treaty Organization, 2020, Pre-ministerial press conference by NATO Secretary General Jens Stoltenberg, Bruxelles (Belgio).

[7] Nel Rapporto NATO 2030 pubblicato nel novembre 2020, si specifica che le nuove tecnologie emergenti e disruptive (EDT) cambieranno la natura della guerra e permetteranno nuove modalità di attacco con missili ipersonici e operazioni ibride.

riscontrati con l'avvio dell'era nucleare. Una significativa area di convergenza è quella delle tecnologie genomiche con l'intelligenza artificiale (AI), l'automazione, la robotica, e il *cloud computing*.

Gli sviluppi nelle tecnologie genomiche e in altre tecnologie emergenti, in particolare *machine* e *deep learning*, sollevano qualche timore nella misura in cui l'accesso ad un'ingente disponibilità di genomi umani, spesso con dati clinici direttamente associati, può implicare la possibilità che dei bioinformatici possano iniziare a mappare la suscettibilità alle infezioni in popolazioni specifiche, come ha sottolineato un rapporto dell'Istituto dell'ONU per la ricerca sul disarmo[8]. Il medesimo studio sottolinea non solo che tali informazioni possono essere usate per lo sviluppo di armi "mirate" a particolari gruppi, ma anche che il *machine learning* applicato all'ingegneria proteica può avere profonde implicazioni nell'identificare possibili bioregolatori e tossine impiegabili per finalità ostili.

Inoltre, con l'espansione del processo di digitalizzazione della biologia, la biotecnologia sta uscendo dai propri tradizionali settori di elezione: l'ingegnerizzazione deliberata della biologia sta aprendo opportunità senza precedenti per l'uso di biomateriali e biocombustibili, sia per l'agricoltura che per la filiera agro-alimentare, oltre che ad esempio per l'ambito energetico. Con l'evoluzione costante delle biotecnologie, sarà la cyber-biosicurezza a dover essere attentamente considerata in relazione alle esistenti infrastrutture critiche connesse a tali settori, mentre nuove componenti di infrastrutture critiche potrebbero emergere ed essere definite tramite i progressi registrati nell'industria della biologia di sintesi[9].

La cyber-biosicurezza è stata associata a vulnerabilità insite nell'intersezione tra cybersecurity, sicurezza cyber-fisica, e biosicurezza – con crescenti applicazioni nell'ambito delle scienze della vita, specie nei settori biomedico e farmaceutico – secondo

[8] United Nations Institute for Disarmament Research, 2020, *Advances in Science and Technology in the Life Science*, Ginevra (Svizzera).

[9] Molti settori afferenti alle infrastrutture critiche possono essere interessati e, di conseguenza, dover svolgere un ruolo nell'assicurare adeguati standard di cyber-biosicurezza. I settori sono quello chimico (in particolare a causa della convergenza fra biologia e chimica), quello dell'industria della difesa, nonché quelli dei servizi di emergenza, dell'energia, dell'alimentazione e agricoltura, della sanità pubblica e delle tecnologie dell'informazione.

una definizione preliminare fornita già nel 2018 da una prospettiva di sicurezza da Murch e altri esperti[10].

A causa della maggiore dipendenza dei diversi settori delle scienze biologiche dai sistemi cyber-fisici, vi sono margini di manovra in ogni punto in cui processi o servizi bioingegnerizzati si interfacciano con il dominio cyber e fisico. In tal modo, attori con intenzioni ostili possono sfruttare reti non protette e manipolare in remoto dati biologici, utilizzare a proprio vantaggio agenti biologici o influenzare l'elaborazione fisica che coinvolge materiali biologici, al punto da provocare, più o meno intenzionalmente, conseguenze indesiderate o pericolose. Oltre ad un potenziale impatto che mette in pericolo la salute pubblica, l'ambiente, l'economia e la sicurezza nazionale, la gamma di rischi e minacce che ne deriva può includere il furto di informazioni per scopi militari e di proprietà intellettuale nel contesto di scenari di guerra economica.

I rischi includono la possibilità di attacchi su sistemi bioinformatici automatizzati, sulle catene di rifornimento biotech, oppure sull'infrastruttura strategica di cyber-biosicurezza. *Malware* di intelligenza artificiale potrebbero essere utilizzati per automatizzare una manipolazione di dati con l'intento di falsificare o sottrarre informazioni all'interno di vaste raccolte di dati genomici.

I cyber-attacchi stanno diventando prevalenti nell'industria delle scienze della vita. Le minacce cyber colpiscono specialmente le grandi aziende farmaceutiche, fenomeno riscontrabile anche prima dell'attuale pandemia. Ma – come è stato sottolineato dall'esperta britannica Kathryn Millett – ad essere interessate potrebbero anche essere le *start-up* del settore biotech, rispetto alle quali non vi sono molti dati disponibili né esistono requisiti formali di reporting[11].

[10] Di conseguenza, la nozione di *cyberbiosafety* è stata introdotta collegandola a vulnerabilità informatiche associate ai sistemi di dati in rete, alle apparecchiature di laboratorio e alla sicurezza delle strutture, nonché ai controlli tecnici che possono provocare contaminazione ambientale o rappresentare una minaccia per la salute degli esseri umani, degli animali e delle piante, compresa la salute della comunità e/o degli utenti e dei consumatori di prodotti creati dalle imprese operanti nel settore delle scienze della vita. Mueller, 2020, *Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?*, Biosafety and Health.

[11] Smith, 2020, *Biotech Startups Face a Growing Wave of Cyberattacks*, Labiotech.eu

***Proposta di strategie***

La pianificazione strategica nazionale, in un quadro europeo e NATO, dovrebbe prevedere un programma volto ad identificare e valutare i rischi in termini di cyber-biosicurezza, in grado di identificare nuove minacce, vulnerabilità, e conseguenze (ad esempio, quelle associate alla biologia di sintesi dal duplice impiego civile e militare, alla proprietà intellettuale nel settore biologico, o alla bioeconomia). Tale programma non potrà che risultare da partnership pubblico- private, con una rilevante partecipazione della Difesa e di altri enti governativi: considerando le ingenti risorse indirizzate ai settori cyber, biologico e all'ambito emergente che promana dalla loro convergenza, ma anche le non sufficienti capacità delle imprese di proteggersi dall'ampia gamma di rischi alla sicurezza, i governi nazionali dovrebbero collaborare con i rispettivi settori privati per definire standard volontari per la cyber-biosicurezza. Un controllo diretto o indiretto della Difesa sugli standard di cyber-biosicurezza adottati dalle infrastrutture strategiche nazionali, inoltre, dovrebbe essere stabilito e perimetrato in coordinamento con la Presidenza del Consiglio in base all'evoluzione del quadro di minaccia.

In questo contesto, il comparto della Difesa potrebbe dover assorbire risorse umane ed *expertise* di tipo scientifico e tecnologico che lo metta nelle condizioni di comprendere lo stato dell'arte negli ambiti cyber e biologico, l'impatto della loro convergenza, gli esiti degli investimenti in tali aree, e le modalità con cui possono impattare sulla sicurezza nazionale[12]. Un tale processo di adeguamento in termini di reclutamento di personale specializzato si metterebbe in moto con l'introduzione di dedicati moduli di *training* nell'offerta formativa degli Istituti di formazione della Difesa, in stretta sinergia con la Scuola di Formazione del Comparto Intelligence in capo alla Presidenza del Consiglio.

A fronte di un ventaglio di fonti di rischio differenti e molteplici, occorre disporre di un'organizzazione strategica di "*biodefense*" rispetto ai rischi biologici emergenti, di cui la Difesa dovrebbe essere uno dei pilastri, considerando anche il ruolo di primo piano che ha assunto sia nel contributo fondamentale della sanità militare e della logistica nel far fronte sin dalle prime fasi all'emergenza sanitaria, sia successivamente nella gestione della campagna vaccinale.

[12] Asha, 2019, *The national security implications of cyberbiosecurity*,, Frontiers in Bioengineering and Biotechnology.

La reazione riscontrata e la tipologia di strumenti e mezzi messi in campo in diversi Paesi per far fronte alla pandemia da SARS-CoV-2, peraltro, ha confermato che non vi è alcuna differenza sostanziale nell'attivazione dei meccanismi di preparazione e risposta alle minacce biologiche emergenti, tenuto conto dell'ampio spettro di sorgenti di rischio che potranno affacciarsi in futuro, siano esse di origine naturale, accidentale o intenzionale.

In un'ottica di "One Health"[13], la sorveglianza delle infezioni umane e animali dovrebbe integrare quella delle patologie vegetali, in particolare per la rilevanza che esse possono avere in scenari di agroterrorismo, il quale rientra nell'ambito del bioterrorismo ed è associato all'introduzione deliberata di agenti patogeni animali o vegetali con l'obiettivo di generare panico, causare danni economici e minare la stabilità sociale. Gli strumenti di sorveglianza dovrebbero essere orientati in particolare sulle capacità di diffusione di specie invasive provenienti da altri continenti, per effetto della globalizzazione.

A tal fine, appare appropriato sviluppare approcci altamente innovativi volti a scongiurare eventi biologici ad alto impatto, con conseguenze sulla salute pubblica, la sicurezza e la stabilità economica nazionale, simili a quelle causate dalla recente pandemia da SARS-CoV-2. La sorveglianza si deve articolare in un monitoraggio dei rischi nonché nell'individuazione di eventuali focolai epidemici "significativi", cioè le cui caratteristiche di patogenicità e trasmissibilità rispondano a ben definiti parametri avvalendosi di attività sia di intelligence dedicate (sul web e sui social), sia di ricerca scientifica finalizzata con *modeling*, al fine di classificare tempestivamente, dal punto di vista genetico, i microrganismi di interesse. I sistemi di bio-sorveglianza in tempo reale devono essere associati ad algoritmi predittivi di epidemie e pandemie con l'ausilio di indicatori precoci di tali eventi prima che raggiungano uno stadio in cui può essere difficile il contenimento. La fase di prevenzione si attiva nel momento in cui i sistemi di sorveglianza rilevano la comparsa di un focolaio in espansione, la cui rilevanza viene assegnata sulla base di indicatori prestabiliti (ad esempio, il numero dei casi, la tipologia

[13] L'approccio "One Health" è promosso e sostenuto dall'Organizzazione Mondiale della Sanità, dalla FAO e dall'Organizzazione Mondiale della Sanità Animale e riconosce come la salute degli esseri umani sia indissolubilmente legata e connessa a quella degli animali e dell'ambiente.

di trasmissione interumana, la genetica del microrganismo, la disponibilità di farmaci/vaccini, nonché il fattore R0, ossia il numero di riproduzione di base).

Per la sorveglianza integrata delle minacce biologiche emergenti il ruolo dell'intelligence, in particolare, si rivelerà sempre più strategico e dovrà favorire un coinvolgimento attivo di attori come quelli della salute pubblica e della salute pubblica veterinaria, il settore industriale nonché il mondo accademico e della ricerca in un'ottica autenticamente multidisciplinare. Nell'ambito della Difesa, tale sorveglianza attraverso gli strumenti e le metodologie descritti – che vanno al di là delle attività convenzionali di *medical intelligence*[14] – potrebbe essere realizzata da una struttura centrale di raccordo tra il II Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa e l'Ispettorato Generale della Sanità militare.

---

MASSIMO AMOROSI, docente presso la Luiss Guido Carli e già consulente per il MAECI sulla non proliferazione CBRN e la biosicurezza, è l'esperto CBRN e di minacce biologiche di RAIT88 e collabora con il Centro Innovazione Difesa dello SMD.

---



[14] Con "Medical Intelligence" ci si riferisce ad un'attività, effettuata prevalentemente in Paesi terzi, finalizzata ad acquisire la disponibilità di informazioni sanitarie accurate da utilizzare sia nel corso della fase di pianificazione dell'operazione, sia in quella successiva di dispiegamento delle forze. Aquino, 2017, *Medical Intelligence*, Informazioni della Difesa.