ieee.es
Instituto Español de Estudios Estratégicos

Opinion Paper

10/2025 06/02/2025

*Alberto Cique Moya**

Confidentiality and Transparency in Security, Defense and Biosecurity: A Critical Balance

Visit webpage Receive Newsletter

Confidentiality and Transparency in Security, Defense and Biosecurity: A Critical Balance

Abstract:

In the world we live in, it is necessary to address the need to balance confidentiality and transparency in the fields of security, defense, and biosafety. The indiscriminate disclosure of operational protocols and scientific advancements can compromise public and national security by providing sensitive information to malicious actors. Examples include access to CBRN (Chemical, Biological, Radiological, and Nuclear) capabilities of security forces, which could be exploited to evade investigations or maximize the impact of attacks.

In the military field, the disclosure of tactics and operational capabilities would reduce strategic and operational advantage, while in biosafety, the dissemination of biocustody measures or dual-use research increases the risk of bioterrorism or misuse. The ethical dilemma revolves around promoting scientific advancements without compromising security, as seen in controversial experiments on gain of function or genetic manipulation through gene drives such as the CRISPR technique.

Keywords:

Security, Defense, Biosecurity, Biosafety, Information, Intelligence, Risks, Vulnerability.

How to quote:

CIQUE MOYA, Alberto. *Confidentiality and Transparency in Security, Defense and Biosecurity: A Critical Balance*. Opinion Paper IEEE 20/2025. web link IEEE and/or link bie[3] (accessed on the web day/month/year)

***NOTE:** The ideas contained in the Opinion Papers shall be responsibility of their authors, without necessarily reflecting the thinking of the IEEE or the Ministry of Defense.

Introduction

In business, «absolute truth» and «total transparency» are considered by some as guarantees of success, this may not be applicable in other areas, especially those related to security and defense[1].

In these contexts, indiscriminately sharing information could not only expose our strengths but also our vulnerabilities. This risk is particularly relevant in dual-use research, where legitimate scientific or technological advancements could be misused for malicious purposes if they fall into the wrong hands. The situation can become even more complex, or at least aggravated, by the advancements and use of Artificial Intelligence (AI) tools, such as deep learning models or large language models (DL or LLMs) [2,3,4].

To clarify this assertion, we only need to imagine someone's intent on committing an illegal act gaining knowledge of the research methodologies and protocols of the Security Forces (Cuerpos y Fuerzas de Seguridad, CFS). Such knowledge could enable them to identify and exploit potential weaknesses in these protocols, successfully evading an investigation after committing a crime[5,6].

To support this argument, consider the scenario where the protocols and capabilities of the intervention units of the Security Forces were public. This would mean that non-state actors could access information about the protective capabilities of police equipment, granting them a tactical advantage that would not only compromise the safety of

All sources have been consulted on December 30, 2024

1 DALIO, R. (2024) «*Confianza en la verdad radical y la transparencia radical*» Disponible en: https://www.principles.com/principles/f6412dca-b3f9-4dd0-bb65-274869dd21ed

2 GREENFIELDBOYCE, N. (2018) «*Did Pox Virus Research Put Potential Profits Ahead of Public Safety? NPR* [pag. web] Disponible en*:* https://www.npr.org/sections/health-shots/2018/02/17/585385308/did-pox-virus-research-put-potential-profits-ahead-of-public-safety?t=1541692661239

3 WORLD HEALTH ORGANIZATION (2020). *What is dual-use research of concern?* World Health Organization [pag. web] Disponible en: https://www.who.int/news-room/questions-and-answers/item/what-is-dual-use-research-of-concern

4 SOICE, EH, ROCHA, R, CORDOVA, K, SPECTER, M, & ESVELT, KM (2023). «*Can large language models democratize access to dual-use biotechnology?* (preprint)» https://doi.org/10.48550/arXiv.2306.03809

5 MORENO BLASCO, S. (2022) «*Táctica Operativa Policial. La seguridad en los controles de tráfico».* Trabajo Fin de Grado, Universidad de Salamanca, Curso de Adaptación al Grado de Criminología, Salamanca. Universidad de Salamanca: [pag. web] Disponible en: https://gredos.usal.es/bitstream/handle/10366/151056/TG_MorenoBlasco_T%C3%A1ctica.pdf?sequence=1&isAllowed=y

6 DEPOL (2023) «*Ascenso Inspector Jefe: Análisis supuesto*» DEPOL [pag. web] Disponible en: https://de-pol.es/wp-content/uploads/2024/09/RESOLUCION_PREGUNTA_2_SUPUESTO_INSPECTOR_JEFE_21SEP2024_DEPOL_Ascenso.pdf

personnel but also reduce police effectiveness, directly affecting public safety[7,8].

Delving further into this issue, if a non-state actor were to learn the operational procedures of the TEDAX-NRBQ (HAZMAT Bomb Disposal) units, they could use this knowledge to maximize the impact of an attack. Furthermore, if they were aware of the detection and identification capabilities for nuclear, radiological, biological, and chemical (NRBQ) agents or substances, this information could be exploited to achieve their goals.

From a defense perspective, this issue could also extend to the Armed Forces. If an adversary were to gain knowledge of our Tactics, Techniques, and Procedures (TTPs) or possess detailed information about our military capabilities in general—or specifically in the NBQ defense domain (considered synonymous with NRBQ)—they could use this knowledge to gain a strategic, operational, or tactical advantage.

When applied to biological risks, understood as the overall probability of harm occurring and the severity of such harm caused by a biological agent or toxin due to unintentional exposure, accidental release or loss, theft, misuse, diversion, unauthorized access, or intentional unauthorized release[9], it seems reasonable to consider establishing safeguards to reduce these risks to acceptable levels and enhance our "biosecurity" in the broadest sense of the term.

An added challenge we face, which undoubtedly complicates matters further, is that "biosecurity" in Spanish has been and continues to be widely used as a synonym for two concepts that are clearly defined in English: biosafety and biosecurity [10]:

- Biosafety refers to preventive measures designed to protect people, the environment, and laboratory workers from accidental risks associated with handling hazardous biological agents. In other words, biosafety is more related to

7 TEJERO, R., & DORAL, N. (2017) «*Black Block: así es el manual de terrorismo callejero que manejan los violentos de la CUP para el 1-O*» OK diario. Disponible en*:* https://okdiario.com/espana/black-block-asi-manual-terrorismo-callejero-manejan-violentos-cup-1-1361774

8 CAÑIZARES, M. (2019). *Técnicas anarquistas de manual para provocar el caos en Barcelona*. Cronica Global. Disponible en*:* https://cronicaglobal.elespanol.com/politica/20191017/tecnicas-anarquistas-manual-para-provocar-caos-barcelona/437456325_0.html

9 ORGANIZACIÓN MUNDIAL DE LA SANIDAD ANIMAL (2023). Glosario de términos. En O. M. Animal, *Manual de las Pruebas de Diagnóstico y de las Vacunas para los Animales Terrestres, duodécima edición (edición online* Vol. 1, pág. viii). Disponible en*:* https://www.woah.org/fileadmin/Home/esp/Health_standards/tahm/0.04_Glosario_2023.pdf

10 BINDER, MK, WILLIAMS, AM, & SIN, SS. (2023). «*Biosecurity in the Americas: A Regional Threat Assessment.* Washington» D.C.: UNSCR 1540 Implementation Program of the Inter-American Committee against Terrorism, Organization of American States

laboratory safety, the safe handling of biological samples, and the prevention of unintentional incidents. It encompasses the principles and practices for preventing unintentional exposure to biological materials or their accidental release[11].

- Biosecurity (or biocustody) encompasses measures to prevent unauthorized access, misuse, or intentional release of hazardous biological agents or related technologies. It is focused on mitigating deliberate threats, such as bioterrorism or the theft of sensitive biological materials by external actors or individuals exploiting their access to such materials. It also includes policies to limit the misuse of biotechnology, as well as the intangible assets associated with this field[12,13,14].

In relation to those intangible assets—such as know-how—that could be applied for malicious purposes, it is worth noting that they are addressed, albeit indirectly and through a broad interpretation, in Spain's 2021 National Security Strategy, which states: «To protect Spain's interests, it is essential to prevent, detect, and neutralize covert aggressions from abroad aimed at illegally obtaining sensitive information to undermine Spain's international image or conduct acts of interference»[15].

Confidentiality of Operational Procedures

The necessity for investigation and intervention protocols to remain confidential is based on reasons of security, protection of those involved, and ensuring a fair judicial process. In truth, confidentiality is essential to guarantee that investigations are conducted without obstructions, safeguarding both individual rights and the collective interests of society and the state[16,17].

11 MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD (2019). *Orden PCI/168/2019, de 22 de febrero, por la que se publica el Plan Nacional de Biocustodia, aprobado por el Consejo de Seguridad Nacional.*

12 MINISTERIO DE PRESIDENCIA (1997) «*Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo*» BOE-A-1997-11144

13 PÉREZ MELLADO, R. (2016) «*Diseño y mejora de medidas de biocustodia: Un ejercicio de sentido común*» Madrid: Imprenta de la Oficina de información diplomática.

14 CENTRO CRIPTOLÓGICO NACIONAL (2024) *CCN-CERT IA-04/24: Ciberamenazas y Tendencias.* Madrid: Centro Criptológico Nacional [pag. web] Disponible en*:* https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html

15 CONSEJO DE SEGURIDAD NACIONAL (2021). «*Estrategia de Seguridad Nacional 2021*» Departamento de Seguridad Nacional. Disponible en*:* https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

16 FROEHLINGSDORF, J. (2021) «*El secreto de las actuaciones en el procedimiento penal*» [pag. web] Disponible en*:* https://cms.law/es/esp/publication/el-secreto-de-las-actuaciones-en-el-procedimiento-penal

17 LIMBU, D. (2024) «*Ex-spy and daughter will not give evidence in court*» BBC [pag. web] Disponible en*:*

In favor of this confidentiality, it should be noted that providing information about the available detection and identification capabilities of NRBQ agents means revealing critical information about our ability to detect or identify which causal agent is involved in a crime. For example, the ability of operational teams to detect and identify Bacillus anthracis during an incident could lead them to declare that this microorganism was detected, when in reality, what was disseminated may be a phylogenetically related microorganism. This discrepancy could jeopardize—unless a well-founded legal opinion suggests otherwise—the subsequent police and judicial investigation[18].

On the other hand, in favor of transparency, the confidentiality of operational procedures might lead citizens to perceive police actions as disproportionate or insufficiently regulated. Therefore, disclosing operational procedures could contribute to improving public trust in law enforcement.

Additionally, another argument in favor of transparency relates to the idea that knowing operational procedures allows for determining whether established regulations have been violated. This is because, in democratic regimes, the Security Forces (Fuerzas y Cuerpos de Seguridad, FCS) are subject to public oversight and accountability. In this way, the observance of citizens' rights is ensured, aiming to prevent abuses of power[19].

Nevertheless, considering all the above, for the sake of effectiveness, operational procedures must remain confidential. If they were made public, public safety would be compromised, and police effectiveness would be undermined (Fig. 1).

Regarding the defense sector, applying the concept of absolute transparency to argue that Tactics, Techniques, and Procedures should be public cannot be justified with the same reasoning—always taking care not to conflict with what is established by International Humanitarian Law. This is because, the less an opponent knows about the established operational procedures, the greater our tactical and operational advantage.

https://www.bbc.com/news/articles/cn0erdydx0go

18 LUNA, V., KING, D., PEAK, K., REEVES, F., HEBERLEIN-LARSO, L., VEGUILLA, W., CATTANI, J. (2006) «*Bacillus anthracis virulent plasmid pX02 genes found in large plasmids of two other Bacillus species*» *J Clin Microbiol 44*(7), 2366-2377. doi:10.1128/JCM.00154-06

19 MINISTERIO DEL INTERIOR (2020) «*Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad para los delitos de odio y conductas que vulneran las normas legales sobre discriminación*» Ministerio del Interior [pag. web] Disponible en*:* https://www.policia.es/miscelanea/participacion_ciudadana/normativa/Protocolo_actuacion_delitos_odio_07-2020.pdf

MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

GABINETE TÉCNICO

OFICIO

S/REF.: Expediente nº **001-000445**
FECHA: 12 de enero de 2014
ASUNTO: Solicitud del Protocolo de actuación de las UIP

DESTINATARIO: PORTAL DE LA TRANSPARENCIA

En contestación a la solicitud de información efectuada a través del Portal de la Transparencia por con número de expediente arriba referenciado, en el que manifiesta tener interés en conocer el protocolo de actuación de las UIP, este Centro Directivo estima que debe denegarse lo requerido al amparo de lo prescrito en el artículo 14 d) de la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*, puesto que se trata de procedimientos operativos policiales cuya difusión fuera del entorno profesional puede afectar a la seguridad pública al ir en detrimento de la eficacia de futuras actuaciones.

EL DIRECTOR GENERAL

Fig 1: https://www.interior.gob.es/opencms/documentacion/Portal-de-Transparencia/ResolucionesDenegatoriasANTERIORESa2019/001-000445.pdf

At this point, it seems reasonable to establish a balance between the need for transparency and the necessary confidentiality of operational procedures, both for the Security Forces (FCS) and the Armed Forces. The degree of confidentiality depends on the nature of these procedures and the context in which they are applied. In fact, some sensitive protocols should remain confidential to protect public safety, the integrity of interventions, and the development of military operations, while ensuring transparency regarding general policies and the principles guiding police actions, as well as the missions assigned to military units.

If everything discussed confirms the need for a balance between confidentiality and transparency in the areas of security and defense, there is no doubt that this approach could be extrapolated to sensitive information associated with scientific research in its broadest sense. This becomes particularly relevant when applied to biological sciences and biosecurity in its broadest definition, given the rapid pace of advancements occurring in a context lacking governance and with ethically questionable approaches[20,21].

20 MURRAY, TR (2012) «*La ética y la biología sintética: cuatro corrientes, tres informes*» Fundació Víctor Grífols i Lucas. Barcelona. [pag. web] Disponible en*:* https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/46693/1/informe5Eticaylabiolog%C3%ADasint%C3%A9tica.pdf

21 WORLD HEALTH ORGANIZATION (2024) «*WHO Technical Advisory Group on the responsible use of the life sciences and dual-use research: report of the meeting*» Geneva: World Health Organization. [pag. web] Disponible en*:* https://iris.who.int/bitstream/handle/10665/379556/9789240102569-eng.pdf?sequence=1

This is because the unstoppable progress we are witnessing—aimed at improving health, society, or the environment, as in the case of synthetic biology—is accompanied by security risks, both accidental and intentional. For this reason, the World Health Organization has developed a global guidance framework to manage these risks and threats. This framework, known as the Guidance Framework for the Responsible Use of Life Sciences (Technical Advisory Group on the Responsible Use of the Life Sciences and Dual-Use Research - TAG-RULS DUR), focuses on dual-use research (DUR), as well as monitoring advancements, particularly in the fields of Artificial Intelligence and synthetic biology (biodesign) [22].

Confidentiality in the Field of Biosecurity

Taking the premise of the need or convenience of confidentiality further, while broadening and applying it to the field of biosecurity/biocustody, we must ask ourselves: Would it be appropriate to make public the biocustody measures established in a laboratory? Or, from another perspective, would it be advisable to disseminate the results of dual-use research?

- Regarding the first question, disseminating information about the security measures implemented in a laboratory handling or storing biological agents, particularly those classified in groups 3 or 4, would clearly be counterproductive. Sharing such data could facilitate the commission of a criminal act, posing a significant threat to security[23].
- On the other hand, the second question addresses even more complex challenges. The ethical dilemma associated with biosecurity in its broadest sense arises from the need to balance the dissemination of knowledge and scientific progress with the protection of sensitive information, which, if exposed, could compromise security.

  This debate is especially relevant in the context of high-risk experiments, such as gain-of-function research in influenza or coronaviruses, which have generated

22 WORLD HEALTH ORGANIZATION (2024) «*Ethics and governance of artificial intelligence for health. Guidance on large multi-modal models*» World Health organization [pag. web] Disponible en*:* https://iris.who.int/bitstream/handle/10665/375579/9789240084759-eng.pdf?sequence=1&isAllowed=y

23 COMITÉ ESPECIALIZADO DE NO PROLIFERACIÓN DE ARMAS (2021) «*Mapa de la biocustodia 2021*» Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.

significant controversies within the scientific community. The discussions often center around the benefits of publishing such studies versus the potential harm they could cause. The problem we face regarding bioprotection/biocustody is the dilemma that knowledge dissemination cannot—and probably should not—be restricted entirely in the name of security[24].

An example of this is the attempt to restrict the dissemination of the genetic sequence of botulinum toxin "H." The central argument is that, since no antitoxin is available for it, publishing that information could have catastrophic consequences[25,26,27].

In both cases, the discussion revolves around the conflict between advancing knowledge and ensuring security, as well as defense. This highlights the delicate line that must be drawn when disseminating sensitive information in the field of biosecurity in its broadest sense[28,29,30].

Dissemination of Sensitive Information and Increased Vulnerability

It is extremely difficult to establish a clear boundary that defines where correctness begins and ends in relation to the dissemination of information for the sake of security. The more restrictive one is, the more the progress of science will be hindered by limiting the dissemination of knowledge.

This discussion is not new and can be summarized by the intelligence world's aphorism:

24 VALLAT, B. (2006) «*Desastres biológios de origen animal. Papel y preparación de los servicios de sanidad animal y salud pública*» *Rev. sci. tech. Off. int. Epiz., 25*(1):12-14.

25 MARTÍNEZ RON, A. (2013) «*La octava toxina botulínica, otro caso de censura científica*» Cuaderno de Cultura Científica. Disponible en: https://culturacientifica.com/2013/10/17/la-octava-toxina-botulinica-otro-caso-de-censura-cientifica/

26 MACKENZIE, D. (2013) «*New botox super-toxin has its details censored*» NewScientist [pag. web] Disponible en: https://www.newscientist.com/article/dn24398-new-botox-super-toxin-has-its-details-censored/#.Ulv3rRAiy3U?utm_source=NSNS&utm_medium=SOC&utm_campaign=twitter&cmpid=SOC%7CNSNS%7C2012-GLOBAL-twitter

27 BARASH, JR, & ARNON, SS. (2014) «*A Novel Strain of Clostridium botulinum That Produces Type B and Type H Botulinum Toxins*» The Journal of Infectious Diseases *209*(2):183-191. https://doi.org/10.1093/infdis/jit449

28 TESCHKE, K, CHOW, V, BARTLETT, K, & NETTEN, C. (2001) «*Spatial and temporal distribution of airborne Bacillus thuringiensis var. kurstaki during an aerial spray program for gypsy moth eradication*» Environ. Health Perspect*, 109*(1):247-254. doi:10.1289/ehp.0110947

29 NATIONAL RESEARCH COUNCIL (2007) «*Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities».* (TA Committee on a New Government-University Partnership for Science and Security. Committee on Science, Ed.) Washington, D.C. The National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK11499/pdf/Bookshelf_NBK11499.pdf

30 DUPREX, W, FOUCHIER, R, IMPERIALE, M, LIPSITCH, M, & RELMAN, D. (2015) «*Gain-of-function experiments: time for a real debate*» Nat Rev Microbiol*, 13*:58-64. doi:https://doi.org/10.1038/nrmicro3405

«need to know, need to share» The balance between the need to know and the need to share has sparked debates throughout history. In fact, this discussion has been used to justify keeping the general public ignorant throughout the ages by various governments. For instance, statements made in the British Parliament in the late 19th century justified such ignorance with the claim «*The teaching of Geography, sir, is ruinous in its effects on the lower classes. Reading, writing, and arithmetic are relatively safe, but geography invariably leads to revolution*»[31,32].

By analogy, with the advances of the U.S. biological program, the question soon arose about the dissemination of research results. It was considered that national security could be threatened. The proposed solution was to publish and share information useful for public health or agriculture in the interest of scientific progress, while sensitive information was classified as secret[33,34].

This dilemma regarding the unrestricted dissemination of sensitive information has intensified over time as knowledge evolved, techniques became simpler, and costs decreased. A culminating point, as previously mentioned, arose with discussions about gain-of-function experiments and the critical need expressed by the U.S. Biotechnology Office for a mechanism to disseminate sensitive scientific information[35,36].

At this point, it is important to consider that advances in life sciences—such as synthetic biology, genomics, or even neuroscience—are not only transforming the agricultural sector but are also leading to promising research in healthcare, energy, and other sectors that benefit from biotechnology in its broadest sense. These advances also relate to the

31 THE INDEPENDENT (2002) «*Sir Ron Cooke: 'We must assert the importance of geography in the curriculum*'» The Independent. Disponible en: https://www.independent.co.uk/voices/commentators/sir-ron-cooke-we-must-assert-the-importance-of-geography-in-the-curriculum-179715.html

32 PARKER STUART, C. (1867) «*Popular Education (Essay V)».* En: Questions for a Reformed Parliament. London MacMillan and Co. 1867:195

33 MERCK, G. (1946) «*Official Report on Biological Warfare»* Bulletin of the Atomic Scientist*, 2*(7-8):9-11

34 FORRESTAL, J. (1949) «*Statment on Biological Warfare»*. Bulletin of the Atomic Scientists*, 5*(4):104-105.

35 NATIONAL SCIENCE ADVISORY BOARD FOR BIOSECURITY (2013) «*Findings and Recommendations».* National Institute of Health [pag. web] Disponible en*:* https://www.nih.gov/sites/default/files/about-nih/nih-director/statements/collins/03302012_NSABB_Recommendations.pdf

36 KUPFERSCHMIDT, K. (2017) «*How Canadian researchers reconstituted an extinct poxvirus for $100,000 using mail-order DNA» Science* [pag. web] Disponible en*:* https://www.science.org/content/article/how-canadian-researchers-reconstituted-extinct-poxvirus-100000-using-mail-order-dna

development of new military capabilities in the field of personnel protection[37,38]

However, it must be taken into account that some of these materials, technologies, and knowledge, integrated or otherwise, can be intentionally used to harm people, animals, plants, or the environment, potentially threatening national security[39]. For this reason, biosecurity, as outlined in the introduction, is a multidisciplinary effort to identify and mitigate the threat of the intentional misuse of such materials, technologies, and dual-use information and knowledge[40].

Key factors determining how the dissemination of sensitive information can increase our vulnerability are outlined below:

- Unfortunately, disseminating sensitive information can help state and non-state actors develop biological programs that are semi-covert in the former and completely covert in the latter. For example, the "materials and methods" sections of dual-use scientific papers describe, in detail, steps necessary to reproduce experiments. This raises the possibility of misuse, as demonstrated by gain-of-function experiments involving the influenza virus (H5N1) or SARS-CoV-2, as well as published research on de novo synthesis involving polio or poxviruses[41,42,43,44,45].
- The unethical or unauthorized applications of biotechnology—such as the use of gene drives that allow precise editing of DNA—open the door to creating or

37 ASEBIO (2024) «*La biotecnología aplicada a la agricultura, clave frente a desafíos como el hambre, el cambio climático y el crecimiento demográfico*». Asociación Española de Bioempresas (AseBio) [pag. web] Disponible en: https://www.asebio.com/actualidad/noticias/la-biotecnologia-aplicada-la-agricultura-clave-frente-desafios-como-el-hambre

38 ORT URUGUAY. (2024) «*Usos y aplicaciones de la biotecnología en la actualidad*» Universidad ORT Uruguay - Facultad de Ingeniería [pag. web] Disponible en: https://fi.ort.edu.uy/blog/usos-y-aplicaciones-de-la-biotecnologia

39 MORITZ, RL, BERGER, KM, OWEN, BR, & GILLUM, DR. (2020). «*Promoting biosecurity by professionalizing biosecurity A credential system could improve policy and practice*» *Science, 367*(6480), 856-858. doi:10.1126/science.aba0376

40 SATYANARAYANA, K. (2011) «*Dual dual-use research of concern: Publish and perish?*» *Indian J Med Res* (133):1-4

41 JACKSON, RJ, RAMSAY, AJ, CHRISTENSEN, CD, BEATON, S, HALL, D. F., & RAMSHAW, IA (2001). «*Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox*» *Journal of Virology*, 1205 - 1210. doi:https://doi.org/10.1128/jvi.75.3.1205-1210.2001

42 CELLO, J, PAUL, AV, & WIMMER, E. (2002) «*Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template*» *Science, 297*(583):1016-1018. doi:10.1126/science.1072266

43 WIMMER, E. (2006) «*The test-tube synthesis of a chemical called poliovirus*» *EMBO, 7*, S3-S9

44 RESNIK, DB, BARNER, DD, & DINSE, GE. (2011) «*Dual-Use Review Policies of Biomedical Research Journals Biosecurity and Bioterrorism*» *Biodefense Strategy, Practice, and Science, 9*(1):49-54. doi:10.1089/bsp.2010.0067

45 SAMPEDRO, J. (2023) «*Virus para la guerra*» Diario El Pais. Disponible en: https://elpais.com/opinion/2023-02-02/virus-para-la-guerra.html

modifying genetically engineered organisms that could impact humans, animals, or the environment[46,47].

A paradigmatic example is the CRISPR-Cas9-based genome editing of human embryos by Chinese researcher Jiankui He in 2018 to make them resistant to HIV. This research sparked worldwide controversy and continues to provoke heated bioethical debates, especially since the researcher argued that he wasn't wrong, only ahead of his time, because the world wasn't ready for these nascent eugenics experiments[48,49,50,51].

- The free dissemination of genetic sequences of all types of microorganisms increases the likelihood that state and non-state actors can access this sensitive information. This endangers security by leveraging Emerging Disruptive Technologies such as synthetic biology, nanotechnology, or even 3D printing[52]. The proliferation of biotechnology companies capable of manufacturing genetic sequences on demand further exacerbates this risk, as actors could legally acquire genetic fragments and assemble them through reverse engineering. Hence, international controls and global governance mechanisms are crucial to address this threat[53].
- Another consideration is the potential for political or criminal intentionality to disrupt supply chains of critical biological materials, such as those needed for vaccine or gene therapy research. Such disruptions could be exploited to interrupt supplies,

46 WELLERSTEIN, A. (2012) «*Mysteries of the Soviet Biological Weapons Program*. Restricted Area- A Nuclear History» [pag. web] Disponible en: https://blog.nuclearsecrecy.com/2012/07/23/mysteries-of-the-soviet-biological-weapons-program/

47 AINSCOUGHT, MJ. (2022). *Next generation Bioweapons: The technology of Genetic Engineering Applied to Biowarfare and Bioterrorism.* Center Future Warfare Series nº 14. U.S Air Force Counterproliferation Center [pag. web] Disponible en*:* https://irp.fas.org/threat/cbw/nextgen.pdf

48 GÓMEZ-SELLÉS GÁRATE, J. (2019) «*Nacimiento de los dos primeros bebés modificados* genéticamente. Análisis del tratamiento de la noticia en España desde el punto de vista de la comunicación de la ciencia». *ArtefaCToS. Revista de estudios de la ciencia y la tecnología, 8*(2), 53-71. doi:http://dx.doi.org/10.14201/art2019825371

49 ESPINOSA WANG, F. (2022) «*Científicos chinos piden proteger a primeros "bebés CRISPR»* DW [pag. web] Disponible en*:* https://www.dw.com/es/cient%C3%ADficos-chinos-piden-centro-especial-que-proteja-a-primeros-beb%C3%A9s-editados-gen%C3%A9ticamente-del-mundo/a-61045387

50 PRIEGO, L. (2022). «*El creador de los bebés CRISPR, He Jiankui, sale liberado de una prisión china»*. Business Insider [pag. web] Disponible en*:* https://www.businessinsider.es/creador-bebes-crispr-he-jiankui-sale-prision-1039755

51 MCCARTHY, S. (2023). «*El controvertido científico chino He Jiankui propone una nueva investigación de edición genética»*. CNN español [pag. web] Disponible en*:* https://cnnespanol.cnn.com/2023/07/03/controvertido-cientifico-chino-he-jiankui-investigacion-edicion-genetica-trax

52 ADAMALA, KP, AGASHE, D., BELKAI, Y, MATIAS DE C. BITTENCOURT, D, MATTHE, YC, et al. (2024). «*Confronting risks of mirror life»*. *Science*. 386(6728):1351-1353 doi:10.1126/science.ads9158

53 KOPLIN, JJ, SKEGGS, J, GYNGE, C. (2022) «*Ethics of Buying DNA» Bioethical Inquiry, 19*, 395–406. doi:https://doi.org/10.1007/s11673-022-10192-w

increasing vulnerability during pandemics or biological emergencies. This underscores the importance of safeguarding strategic independence[54].

- When discussing the creation of known biological agents—or even chimeras—it's important to note the possibility of introducing antibiotic or antiviral resistance genes or modifying surface antigenic determinants to evade established diagnostic techniques. This would undoubtedly heighten global health security threats[55]. However, the unrestricted dissemination of genetic sequences during the early stages of an outbreak—whether epidemic or pandemic—can allow research teams to develop diagnostic tools or vaccines against the agent in question. For example, the rapid dissemination of SARS-CoV-2 sequences enabled the development of diagnostic tools in a short time frame.
- Additionally, in the interest of security and economic interests, technical and design details—along with information about the biological agents being worked on in biological and biopharmaceutical research facilities—must be safeguarded. These facilities legitimately invest in research and development programs that should undoubtedly be protected, provided they do not violate the Biological and Toxin Weapons Convention.

  This issue becomes even more complex in light of the existing debate regarding the origin of the SARS-CoV-2 virus, highlighting the need to maintain secrecy, especially since no verification tools currently exist, and confidence-building measures are insufficient to foster collaboration with some countries considered proliferators by others[56,57]. Furthermore, research facilities—whether basic, applied, or reference laboratories—are vulnerable to cyberattacks, sabotage, or direct attacks[58].

54 BORRELL, J. (2020) «*Por qué es importante la autonomía estratégica europea*» European Union External Action [pag. web] Disponible en: https://www.eeas.europa.eu/eeas/por-qu%C3%A9-es-importante-la-autonom%C3%ADa-estrat%C3%A9gica-europea_es

55 GALATAS, I. (2017) «*The misuse and malicious uses of the new biotechnologies*» *Annales des Mines - Réalités industrielles*, 10.3-108.

56 TUCKER, JB. (2013) «*The Current Bioweapons Threat*» En: H. e. al.(Ed.), *Biopreparedness and Public Health: Exploring Synergies* (págs. 7–16). NATO Science for Peace and Security Series A: Chemistry and Biology. doi:10.1007/978-94-007-5273-3_2

57 DELEGATION OF THE EUROPEAN UNION TO THE UN AND OTHER INTERNATIONAL ORGANISATIONS IN GENEVA (2023) «*Position of the European Union - Compliance with and verification under the Biological and Toxin Weapons Convention*» Delegation of the European Union to the UN and other international organisations in Geneva [pag. web] Disponible en: https://www.eeas.europa.eu/delegations/un-geneva/position-european-union-compliance-and-verification-under-biological-and-toxin-weapons-convention_en?s=62

58 HORTON, J. (2023) «*Sudan crisis: WHO warns of biological hazard at seized lab*» *BBC* [pag. web] Disponible en: https://www.bbc.com/news/world-65390285

- From another perspective, the risks and threats associated with biotechnological techniques and applications in biodiversity and ecosystems cannot be overlooked. For instance, publishing research on environmental bioengineering—ranging from pest eradication to crop modification or the uncontrolled release of vector arthropods to combat diseases—could cause harm to biodiversity.

  Hence, compliance with the Convention on Biological Diversity is essential, as it covers «the transboundary movement, transit, handling, and use of all living modified organisms that may have adverse effects on the conservation and sustainable use of biological diversity, taking into account risks to human health»[59].

Conclusions

The dissemination of sensitive information in the field of biological sciences can increase vulnerability at various levels: from global security and ecosystem stability to public health. The dual nature of biotechnology—capable of generating both advancements for the benefit of humanity and being used destructively—underscores the need for strict regulation and controlled dissemination of information to minimize risks. The release of such data must carefully balance the pursuit of scientific transparency with the protection of security and bioethics.

In critical contexts such as security, defense, and biosecurity, striking a balance between transparency and confidentiality is essential. While transparency promotes accountability and the advancement of knowledge, the disclosure of sensitive information can lead to severe risks, such as operational vulnerabilities or threats to public health.

In biosecurity, the handling of research such as "gain-of-function" experiments or the development of gene-editing tools (e.g., CRISPR) illustrates the complexity of the dilemma. While the dissemination of knowledge is crucial for scientific progress, there is a danger that this information could be misused—for instance, in the development of biological weapons.

History has shown that both absolute transparency and extreme confidentiality are

59 SECRETARÍA DEL CONVENIO SOBRE LA DIVERSIDAD BIOLÓGICA (2000) «*Protocolo de Cartagena sobre Seguridad de la Biotecnología del Convenio sobre la Diversidad Biológica: texto y anexos».* Montreal.

problematic in the realm of science. It is imperative to adopt an ethical approach that evaluates each case individually, weighing the benefits and risks of sharing information. Public policies must strike a middle ground, ensuring the protection of both collective security and democratic principles, especially when dealing with sensitive information in dual-use research.

The tension between transparency and confidentiality has no universal solution. However, a balanced approach that prioritizes risk assessment and ethical impact may offer a viable way forward. It is crucial to ensure that decisions about what information to share and what to protect are based on clear ethical principles and a rigorous evaluation of potential consequences.

The advancements of Emerging Disruptive Technologies, such as synthetic biology and Artificial Intelligence, among others, represent an emerging threat. This necessitates the establishment of an ethical and regulatory global governance framework to mitigate the risks arising from science and technology.

Alberto Cique Moya
Veterinary Colonel - Military Health Corps
Joint Health Directorate – Joint Defense Staff
Full Member of the Royal Academy of Veterinary Sciences of Spain)