Protecting Global Health in the Americas: Cybersecurity and International Collaboration

Gaudys L. Sanclemente

Protecting Global Health in the Americas: Cybersecurity and International Collaboration

Editorial FLACSO Ecuador

FLACSO Ecuador, Quito

Published 2025
Printed in Ecuador

ISBN: 978-9978-67-704-9 (print)
ISBN: 978-9978-67-705-6 (pdf)

https://doi.org/10.46546/2025-64atrio

FLACSO Ecuador
La Pradera E7-174 and Diego de Almagro, Quito, Ecuador
Tel.: (593-2) 294 6800 Fax: (593-2) 294 6803
www.flacso.edu.ec

Cover art: Antonio Mena

Sanclemente, Gaudys L.

Protecting global health in the Americas : cybersecurity and international collaboration / Gaudys L. Sanclemente.- Quito, Ecuador : FLACSO Ecuador, 2025

xv, 326 pages: illustrations, figures, tables . - (ATRIO Series)

ISBN: 9789978677049 (print)
ISBN: 9789978677056 (pdf)
https://doi.org/10.46546/2025-64atrio

Bibliographical references: pp. 292-325

PUBLIC HEALTH; COVID-19 (DISEASE); PANDEMIC;
PUBLIC POLICIES; INTERNATIONAL COOPERATION;
COMPUTER SECURITY; DATA PROTECTION; HEALTH ASPECTS

362.10684 - CDD

A The Atrio Series is comprised of peer-reviewed works.

Without you, I am but a whisper,
With you, I rise, I soar.
You're the beacon that guides my way,
The bedrock, steadfast and secure.
I dedicate this work with love.

To my dear parents, Rosa and Santiago Sanclemente

Contents

Illustrations

Figures

Tables

Abbreviations

ABR	Antibacterial Resistance
AI	Artificial Intelligence
AMR	Antimicrobial Resistance
AMRO	Regional Office for the Americas
ANLIS	Administración Nacional de Laboratorios e Institutos de Salud "Dr. Carlos Malbrán"
ANT	Actor-network Theory
APUA	Alliance for the Prudent Use of Antibiotics
ARDS	Acute Respiratory Distress Syndrome
BRICS	Brazil, Russia, India, China and South Africa
CAESAR	Central Asian and European Surveillance of Antimicrobial Resistance
CAGR	Compound Annual Growth Rate
CARB	Combating Antibiotic-Resistant Bacteria
CARSS	China Antimicrobial Resistance Surveillance System
CDC	Centers for Disease Control and Prevention
CHINET	China Antimicrobial Surveillance Network
CISA	Cybersecurity and Infrastructure Security Agency
CNP	Collaborative network path [inclusive of paths A, B, C, and D]
COVID-19	Coronavirus Disease 2019
CWMD	[office for] Countering Weapons of Mass Destruction

DACOS	Deputy Assistant Chief of Staff
DHS	Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNA	Deoxyribonucleic acid
EARS-Net	European Antimicrobial Resistance Surveillance Network
ECDC	European Centre for Disease Prevention and Control
EMTs	Emergency medical teams
FAO	Food and Agricultural Organization
FDA	Food and Drug Administration
GAP-AMR	Global Action Plan on Antimicrobial Resistance
GARDP	Global Antibiotic Research and Development Partnership
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
GHSA	Global Health Security Agenda
GLASS	Global Antimicrobial Resistance Surveillance System
HHS	[U.S. Department of] Health and Human Services
HITS	Hyperlink-induced topic search
HIV	Human Immunodeficiency Virus
HIV/AIDS	Human Immunodeficiency Virus / Acquired Immunodeficiency Syndrome
ICT	Information and Communication Technologies
ICU	Intensive Care Unit
IESS	Instituto Ecuatoriano de Seguridad Social (Ecuadorian Social Security Institute)
IHR	International Health Regulations
INSPI	Instituto Nacional de Investigación en Salud Pública (National Institute for Public Health Research)
ISSFA	Instituto de Seguridad Social de las Fuerzas Armadas (Social Security Institute of the Armed Forces)
ISSPOL	Instituto de Seguridad Social de la Policía Nacional (Social Security Institute of the National Police)
IUTLD	International Union Against Tuberculosis and Lung Disease

MERS-CoV	Middle East Respiratory Syndrome Coronavirus
MIC	Minimum inhibitory concentration
MRSA	Methicillin-resistant Staphylococcus aureus
NATO	North Atlantic Treaty Organization
NBIC	National Biosurveillance Integration Center
NCC	National Coordinating Center
NFP	National Focal Point
NGO	Non-Governmental Organization
NRL	National Reference Laboratory
OECD	Organization for Economic Cooperation and Development
OSINT	Open-source intelligence
PACCARB	Presidential Advisory Council on Combating Antibiotic-Resistant Bacteria
PAHO	Pan American Health Organization
PDF	Portable Document Format
PEW	Pew Charitable Trusts
PHEIC	Public Health Emergency of International Concern
RATs	Remote Access Trojans
R&D	Research and Development
REDNARBEC	Red Nacional de Vigilancia de Resistencia Bacteriana del Ecuador (National Bacterial Resistance Surveillance Network of Ecuador)
ReLAVRA	Red Latinoamericana de Vigilancia de la Resistencia a los Antimicrobianos (Latin American Network for Antimicrobial Resistance Surveillance)
RPI	Rensselaer Polytechnic Institute
SARS	Severe Acute Respiratory Syndrome
SITREP	Situation Reports
SIVE	Sistema Integrado de Vigilancia Epidemiológica (Integrated Epidemiological Surveillance System)
SOSIG	Social Science Information Gateway
STAG-AMR	Strategic and Technical Advisory Group for Antimicrobial Resistance
STS	Science and Technology Studies

TAGISAR	Technical Advisory Group on Integrated Surveillance of Antimicrobial Resistance
TB	Tuberculosis
UN	United Nations
URL	Uniform Resource Locator
USAID	United States Agency for International Development
USAMRID	U.S. Army Medical Research Institute of Infectious Diseases
WEKA	Waikato Environment for Knowledge Analysis
WHA	World Health Assembly
WHO	World Health Organization
WOAH	World Organisation for Animal Health
WTO	World Trade Organization

Acknowledgments

I thank God for his abundant blessings, and the archangels whose quiet wings stirred the winds that carried this book to life. I also extend my deepest thanks to my parents, whose encouragement and enduring belief in me have been a wellspring of strength throughout this journey.

I am sincerely grateful to Dr. María Belén Albornoz and Dr. Fredy Rivera Vélez for their generous guidance, intellectual direction, and steadfast support. Special thanks also to the interviewees whose time and perspectives contributed to the depth of this study, and to the peer reviewers for their thoughtful feedback.

My appreciation extends to the Department of International Studies and Communication, the CTS Lab (Science, Technology, and Society Laboratory), and the Strategic Studies Research Group at FLACSO Ecuador (Latin American Faculty of Social Sciences) for their academic and intellectual encouragement throughout this research process.

I am also grateful to the institutions whose publicly accessible materials and general information supported aspects of this research. These include the United States Department of Defense, United States Army, United States Special Operations Command, the Centers for Disease Control and Prevention, the World Health Organization, and The Pew Charitable Trusts. Their contributions added valuable perspective and were instrumental in shaping a more nuanced understanding of the broader dimensions explored in this research.

Finally, I offer sincere thanks to Editorial FLACSO Ecuador and its design team. Your care, precision, and creative collaboration in producing this book with clarity and purpose leaves an imprint I will always cherish.

Introduction

> I saw a large river meandering slowly along for miles, passing from one country to another. I saw huge forests, extending along several borders. And I watched the extent of one ocean touch the shores of separate continents. Two words leaped to mind: commonality and interdependence. We are one world.
>
> —John-David Bartoe

The Walls

When individuals recognize the significance of time and are confronted with the task of conducting research and writing amidst a pandemic, their entire perspective on life undergoes a profound shift. Nevertheless, they persevere in the face of adversity. Similarly, civil society experienced a gamut of emotions as the walls of social distancing swiftly emerged, national borders closed, and countries entered into lockdown, encompassing global measures.

Wall of dismissal
Wall of smugness
Wall of arrogance
Wall of confidence
Wall of aggression
Wall of denial
And then the wall started crumbling.

In 2020, marked by unforeseen events, new and unheralded norms emerged, brought upon by the coronavirus disease (COVID-19) as a public health crisis. The pandemic changed international and domestic relations. It increased tensile forces and caused the foundations of social, political, and economic structures to crumble. From enhanced technology to security challenges, the public and private sectors played crucial parts in providing crisis and emergency-relief responses to the rapidly spreading virus. The coronavirus unleashed tumultuous waves and storms across international borders and forced security providers to go beyond their responsibilities to address the blanket threat of infectious diseases.

Collaboration plays a critical role in ensuring security for civil society. Before the pandemic, security measures were typically implemented on a case-by-case basis within specific industry sectors. In the healthcare industry, the World Health Organization (WHO), under the aegis of participating countries, territories, and areas, collaborates on global health with diverse actors interconnected through the support of relevant players with a common interest. Meetings by nation-states, institutions, industry leaders, and the ministries of health were held between 2015 and 2021 to discuss strategies for combating antimicrobial resistance (AMR). However, with the rampant and unexpected global influx of COVID-19, emergency meetings were held by delegates and think tanks from various industries to tackle the new threat.

As a result, two global threats forced actors to address and tackle the issues simultaneously. In 2020, the Presidential Advisory Council on Combating Antibiotic-Resistant Bacteria (PACCARB) held a virtual meeting focused on the impact of COVID-19 and its effect on AMR. This dual challenge underscores the necessity of collaboration and the importance of shared governance mechanisms, specifically the *security governance of infectious diseases and data sharing through surveillance systems,* in addressing emerging threats.

Governance of security to contain and manage infectious diseases is crucial on a national and global scale to ensure accountability in responding to the crisis. For instance, during the pandemic, governments establish rules for the safe handling and management of infectious diseases, such as country lockdowns and advisories on wearing a mask. By fostering collaboration and interconnection, we can effectively address the challenges of infectious diseases and prioritize a healthy society. Interconnectedness and transparency in data sharing are vital in tearing down the emotional walls of confusion and uncertainty.

Who are the actors in the surveillance network of infectious diseases? Are nation-states the influential power players, or do institutions balance the scales by maintaining a significant role in the international system? Interconnectedness and transparency in data sharing play crucial roles in breaking down barriers to information exchange. By establishing robust communication networks and platforms, we can facilitate the exchange of accurate and timely information, promoting a more informed public discourse. Transparency in data sharing ensures that the information disseminated is reliable and supported by evidence. However, prioritizing the safety and security of that information during transmission is essential. Safeguarding data and ensuring the reliability of sources can help build trust and credibility, ultimately leading to a more informed and united response to pandemics.

However, the pandemic has created an intrusive global system. We are well aware of the channels of misinformation on both global and national scales. We understand that change is necessary, yet we find ourselves trapped in a cycle of repetitive questioning. What is the solution? What actions should the key players, as agents of continuity, take? Who are these key players responsible for reducing disinformation and uncertainty? It is time to cease the constant questioning and instead take decisive action towards global health and security. The recurring cycle of uncertainty leads to divisions in various sectors. However, by fostering collaboration and interconnection, we can effectively combat infectious diseases and prioritize a healthy society. When information flows freely and is accessible to all, it creates opportunities for informed decision-making, but it also amplifies the risks of misinformation and confusion if not carefully managed.

By adhering to stringent data protection protocols and implementing robust cybersecurity measures, we can protect the integrity of the information while fostering an environment of collaboration and trust. This ensures that the interconnectedness we strive for is not compromised by malicious actors or the spread of false information. Moreover, promoting responsible and ethical data-sharing practices is essential in this interconnected world, where information travels at unprecedented speeds. Governments, international organizations, scientific institutions, media outlets, and individuals all have a role to play in ensuring the reliability of shared information. By working together and promoting transparency, we can pave the way for a healthier, more secure global future.

Objectives, Core Research Question, and Hypothesis

As individuals reeled from the deadly pandemic, a mutual symbiosis arose, encompassing the interconnection of actors that share resources to keep each other alive. This research is guided by three primary objectives:

1. **Opening the Black Box of a Health Regime:** Illustrating a surveillance system, namely open-source intelligence (OSINT), that monitors infectious diseases. This includes discussing the strengths and weaknesses of instruments that produce *inscriptions*[1] to address cybersecurity, emerging technologies such as artificial intelligence (AI) and high-performance computing, and nontraditional threats such as infectious diseases, algorithms, and biases.

2. **Analyzing Security Governance**: Understanding how the emergence of an unconventional threat activates security governance, promoted by collaborative dynamics, *dispositifs*,[2] and *boundary objects*[3] (Bowker 2001; Star and Griesemer 1989; Latour 1987) based on open information exchange in the Global Antimicrobial Resistance Surveillance System (GLASS),

---

[1] The term *inscription* means a visual display, not as an end goal, but as an intermediary used in the exchange between actors such as groups of researchers and scientists who may have conflicting purposes in arriving at an inscription; an instrument (or inscription device) produces an inscription (Latour 1987).

[2] The term *dispositif* refers to the apparatus such as discourses, institutions, regulatory decisions, laws, or scientific and philosophical statements (Foucault 1980).

[3] The term *boundary object* distinguishes differences while providing common points of reference and consists of scientific objects that inhabit intersections of the social world, information, organizational structure or arrangements, a negotiation process, the mediator between groups, or any concrete element that assists in drawing a boundary between data and policy (Orsini, Louafi, and Morin 2017; Star and Griesemer 1989; Gieryn 1983).

which promotes a health regime for the surveillance of bacteria pathogenic to humans. This objective also emphasizes the role of international collaboration in establishing surveillance instruments of production, data sharing, and monitoring of infectious diseases and AMR.

3. **Explaining the Role of Security Governance**: Demonstrating why security governance facilitates securing a health regime in the surveillance of infectious diseases through OSINT. This involves identifying risks, vulnerabilities, and resources due to the complex ways multiple actors depend on each other for data exchange.

The core research question is: Why did security governance, through the OSINT technology database of the WHO, promote the health regime on the surveillance of communicable diseases in the Americas from 2015 to 2021? The core hypothesis posits that a new contemporary health regime emerges based on security governance to address nonconventional threats. This research measures the perceptions of nontraditional threats in the Americas from 2015 to 2021, focusing on infectious diseases that transcend national borders. Governance of security to protect populations from infectious diseases promotes the emergence of a health regime when countries collaborate through an open-source intelligence database that contributes to harmonizing data sharing in promoting global health. Such governance fosters the health regime when countries remove barriers, collaborate, and interconnect transparently to exchange information.

In terms of academic scope and contribution to knowledge, this research has a distinct identity and investigative nature. Firstly, it identifies the emergence of a health regime through a specific case study focused on the Americas, with the health regime serving as the unit of analysis. Secondly, the academic contribution lies in exploring the establishment of a security regime within this health regime. This interdisciplinary research integrates insights from fields such as security and strategic studies (including cybersecurity and intelligence), global health, international law, sociology of health and technology, and science and technology studies to examine the emergence of a health regime. Expanding on these interdisciplinary contributions, the next section delves into the context and justification of this research, exploring how surveillance systems and collaborative networks shape the health regime.

Presentation of the Research and Justification

Building and maintaining surveillance system databases involve collecting intelligence and sharing information, such as data on AMR at the global level. However, does free information slow down or benefit actors who contribute information toward a common interest? For instance, the WHO provides publicly available data through its GLASS technology database, containing health information on eight bacterial pathogens that infect humans. The WHO declared AMR as one of the top ten critical global public health threats (World Health Organization 2020b, 2017b).

Promoting global health through collaborative efforts enhances the security of countries, facilitates informed decision-making, and drives national, regional, and global actions. Moreover, both abrupt and gradual changes in health status, such as those occasioned by infectious diseases, influence national security. However, significant variations between countries are barriers to global collaborative health research efforts in sharing big data. How do security or privacy protection groups slow down the technological advancement of open-source information, transparency, and data sharing in health care surveillance systems? These challenges emphasize the critical role of collaboration among actors in ensuring the efficiency and security of surveillance networks.

This change underscores a progressive shift in international studies. Traditionally, national security threats were narrowly confined to national boundaries and military challenges. However, infectious diseases transcend borders, ignoring such limitations. Between 2015 and 2021, this study assessed perceptions of nontraditional threats in the Americas, specifically infectious diseases, in relation to the emergence of a health regime driven by collaboration, publicly available information exchange, and harmonized data sharing to promote global health.

Moreover, the WHO declared AMR a global public health problem and indicated its critical nature as a health threat through publicly available GLASS reports (World Health Organization 2020g, 2018a, 2017b). This collaborative process transforms the data into useful intelligence. Such collaborative interconnectedness provides real-time responses by agents of continuity, including policymakers, the military, teams addressing hazards, and teams managing medical emergencies, to reduce strategic surprises. This is essential because communicable diseases transcend national borders and are deeply interconnected.

This interweaving relationship, collaboration, and complex interdependence of countries and institutions occur because of strong net-neutrality regulations versus proxy options for accessing data. Although open-source data in the surveillance of infectious diseases provide collateral material, the data can also be used as a source for illicit activities and large cybercrime campaigns. Pathogens leading to global pandemics affect the economy and global citizens alike while inspiring critical analysis of the role of information exchange in big data and collaborative efforts.

This book proposes that security governance, as a strategic opportunity for intelligence collection, facilitates the emergence of a health regime through information sharing from publicly available data. By analyzing GLASS data, this research examines how countries collaborate within the surveillance network to promote global health and pursue common interests. It is important to note that this investigation does not aim to conduct a controlled research study comparing nation-states, such a study would have proved difficult because of incomplete information provided by most countries regarding the GLASS standards. Instead, the focus is on analyzing how GLASS, as a boundary object, facilitates the connection between countries through a security governance system in the surveillance of infectious diseases. Furthermore, the study investigates how GLASS functions as a supportive mechanism in the development of national surveillance systems and organizational responses to threats, as well as the impact of infectious diseases on the responses of collaborative actors and heightened security measures in the interest of national security.

Since each nation-state addresses security measures differently, governments must tackle the diseases and other variables thrown into the mix. A lack of transparency and inadequate information sharing affect the most vulnerable, limiting access to testing capabilities, creating confusion, heightening civil division, and sparking protests against governments for lack of accountability. The absence of sufficient health and security measures early in combating threats undermines the health, safety, and security of citizens. How governments articulate security is paramount in fighting a pandemic-actor collaboration and interconnectedness are essential. In 2019, the emergence of the coronavirus as a nontraditional threat created an immediate response through the interconnection of actors. This triggered considerations of national security, information intelligence exchange, global health, and open data sharing. The findings of this research contribute to professional fields, academic settings, the global regions such as the North and South, where actors collaborate and interconnect to share data of common interests. To supplement and reinforce the core research topic, a brief analysis of COVID-19 as a research context is included.

Understanding the dynamics of knowledge production and data sharing is crucial, especially in regions where the participation of countries from the global South is limited. Furthermore, this research highlights the interconnected actions of actors collaborating within the GLASS surveillance network, all working toward a shared goal of global health. The pandemic disproportionately impacted diverse groups and industry sectors. Collaboration and interconnectedness are vital for combating future global health threats effectively.

This research underscores the significance of aligning the *security governance of infectious diseases and data sharing through surveillance systems* with global collaborative efforts. By fostering interconnectedness and transparency, this approach aims to mitigate the risks posed by emerging infectious diseases and AMR.

The complexities of security governance in international relations reflect the interplay between state behavior and global collaboration. Addressing nontraditional threats such as infectious diseases, compromised cybersecurity, and emerging technologies requires coordinated action across diverse actors and sectors. These challenges highlight the importance of fostering trust and transparency within global governance mechanisms, particularly when national interests and security concerns intersect with broader public health priorities.

Institutions play a pivotal role in shaping the rules and processes that guide the international surveillance of infectious diseases. By analyzing these mechanisms, this study demonstrates how collaborative frameworks, and shared objectives can promote the emergence of a health regime to mitigate security threats. The alignment of institutional efforts through platforms like GLASS draws attention to the potential for collective action to enhance global health security and respond to emerging challenges.

The analysis of GLASS data in this study examines how countries collaborate within the surveillance network to promote global health and pursue common interests. It is important to consider technological advancements and access to information in less developed countries, as they contribute to the need for knowledge production and data sharing, particularly when countries are in the early stages of development and require support. Overall, understanding the dynamics of knowledge production and data sharing is crucial, especially in regions where the participation of countries from the global South is limited. Further exploration of these factors can provide valuable insights for improving collaboration and strengthening the AMR surveillance efforts in these countries.

While the primary focus of the analysis is on the GLASS surveillance system of infectious diseases, it highlights collaborative efforts to enhance the security of countries and illustrates the interconnected actions of actors working within the network, all striving toward a shared goal of global health. The emergence of COVID-19 as a novel security threat underscores the importance of context, revealing challenges such as data biases and uncertainties that arise when nation-states fail to collaborate. These challenges influence network and security governance, shaping emergency responses and disaster management strategies.

The choice of this research topic was driven by practical considerations, aiming to deepen existing knowledge by facilitating informed decision-making and promoting sustainability. The findings contribute to the body of knowledge and are relevant to multiple stakeholders, particularly in addressing global health concerns linked to the spread of emerging resistance mechanisms that threaten effective treatment of infectious diseases. By framing these challenges within the broader context of collaborative governance, this research emphasizes the innovative potential of collective action in addressing nontraditional security threats.

Innovations: Contributions to Knowledge Production

This research underscores the importance of integrating interdisciplinary perspectives to address global health and cybersecurity challenges of nontraditional threats. By merging these disciplines, the research highlights a nuanced interdisciplinary approach that bridges theoretical frameworks with practical applications in addressing nontraditional threats. By examining governance frameworks and collaborative networks, the study offers innovative insights into how global actors respond to infectious disease challenges. The integration of disciplines including security studies, global health, and science and technology studies provides a comprehensive framework for analyzing security governance in AMR surveillance. Each discipline offers distinct contributions: security studies enhance understanding of collaborative mechanisms, global health contextualizes the urgency of infectious disease management, and science and technology studies drive innovation in data-sharing platforms.

The study encompasses several innovations, such as collaborative approaches that utilize publicly available information and data exchange through surveillance platforms such as GLASS. The reciprocal relationship between the collaborative environment and data sharing represents a unique and essential focus within this research. While fields such as security studies (cybersecurity and intelligence), global health, and science and technology studies are well-established, this research offers a novel integration of these disciplines within the context of security governance and understanding AMR surveillance, providing innovative pathways for informing decision-making and driving global actions based on data. Technological innovation plays a critical role in automating high-volume data tasks, freeing resources to address higher-value threats such as infectious diseases. Through strategic security measures, this innovation supports global collaboration on AMR surveillance and strengthens international preparedness.

In addition, the study disseminates to a larger group of actors the importance of innovative practices such as enhancing diverse ideas between actors and spreading awareness of the potential security risks in information control, control of diseases, data sharing, and the use of open-source. Likewise, the research demonstrates the fundamental role of openly available information in fostering curiosity, innovation, and learning. Consequently, this work offers a fresh perspective on an emerging health regime, emphasizing the role of security considerations in enhancing preparedness and response to infectious diseases. It emphasizes the importance of open data sharing to facilitate collaborative and technological advancements in the field.

This research highlights the innovative value of collective action by global actors, including nation-states, Non-Governmental Organizations (NGOs), and international organizations, in combating infectious diseases. By investigating the interconnections between human and nonhuman actors during 2015-2021, the study demonstrates how collaborative networks enhance monitoring, preparedness, and response to nontraditional threats. To provide a deeper understanding of these collaborative networks and their impact, the following section outlines the theoretical framework that guides this study, connecting interdisciplinary innovations to the governance mechanisms underpinning infectious disease surveillance.

Synopsis of the Theoretical Framework

Which theoretical perspectives best explain and provide insight into why security governance, through the WHO's open-source intelligence technology database, supports a health regime for infectious disease surveillance? This study integrates three key theories–liberal institutionalism, securitization, and actor-network theory (ANT)–to comprehensively analyze international studies. Complementary concepts such as complex interdependence, security governance, and regimes further enrich the analytical framework.

To enhance the analysis, concepts like collaboration, boundary objects, *dispositifs*, and inscription devices are interwoven, serving as anchors and bridges between the theories and concepts. These frameworks provide a comprehensive approach to understanding the roles of various actors within the network. In particular, securitization theory highlights the politics surrounding the collaborative actions of referent objects–those entities deemed vital for survival or protection–which shed light on how specific issues, like infectious diseases, are elevated to matters of security. By connecting these theories, this study explores the dynamics of interaction between actors, fostering a nuanced understanding of security governance in the context of global health.

As global complexities intensify, collaborative work involving diverse actors becomes increasingly vital. While nation-states continue to play a central role in the international system, global health crises such as AMR and COVID-19 have demonstrated the critical contributions of other actors, including data scientists, engineers, and decision-makers. These contributors address transnational challenges that transcend national borders. Although the pandemic revealed moments when nation-states reverted to insular policies, it also highlighted the essential role of collaborative networks and multilevel governance in managing nontraditional threats.

Insights derived from this research build upon theoretical traditions to highlight how collaborative networks involving diverse actors can address complex global health challenges. These perspectives bridge traditional state-centric models with the flexibility required to govern infectious diseases and other transnational threats effectively. By focusing on the interplay between institutional frameworks, securitizing dynamics, and actor-network flexibility, the study illustrates the evolving mechanisms of security governance in response to nontraditional threats.

A health regime can no longer be black-boxed, a notion that demands moving beyond debates that offer little practical value, such as D'Israeli's (1807) rhetorical query, *How many angels can dance on the point of a very fine needle?* As technology evolves and security risks escalate, issues previously relegated to the periphery of the security agenda have surged to the forefront. The dynamic nature of these challenges necessitates the continual expansion of knowledge-based theories and concepts, which evolve in parallel with advancements in technology and emerging threats.

Liberal institutionalism theory provides a framework for incorporating states and institutions in addressing global affairs, emphasizing their collective capacity to tackle complex challenges. Securitization theory, meanwhile, analyzes security governance as a causal mechanism, offering insights into the processes that define securitized issues. Despite its utility, limited literature explores the causal relationships between actor behaviors in this context. Without institutional trust and alignment with the cause, participating countries may hesitate to contribute to frameworks like GLASS, designed to monitor antimicrobial diseases. Additionally, securitization theory highlights the inherent asymmetry of interests between nations regarding infectious diseases and cyberspace, raising critical questions: Can this digital space be governed effectively through regulations and security measures? Such inquiries further the exploration of securitization dynamics.

Furthermore, this research incorporates contributions from the ANT, which offers a valuable theoretical framework for analyzing networks as collaborative security governance mechanisms. Networks provide flexibility, allowing new actors to adapt to collective interests and enabling open communication channels in our complex and interdependent world. The emergence of COVID-19 highlighted how actors such as policymakers, the military, data scientists, researchers, academics, and security personnel collaborated to address unconventional threats. These efforts underscore the importance of the interdisciplinary frameworks and collaborative networks explored in this study, demonstrating their relevance in navigating global health challenges. The theory contributes concepts such as translation, the normalization of the black box, and network analysis and also allows for the exploration of nonhuman actors, including the GLASS technology database and the International Health Regulations (IHR) code of law. These theories collectively form the foundational structure supporting the analysis in this study and contribute to the examination of data and security governance in the matter of pathogens in promoting a health regime within the surveillance of infectious diseases.

By synthesizing the contributions of liberal institutionalism, securitization, and ANT, the study provides a multifaceted lens for understanding security governance. Liberal institutionalism emphasizes how states and institutional actors collaborate to address global challenges, securitization theory analyzes how issues are framed as security concerns through social processes, and ANT examines the interplay between human and nonhuman actors within networks. This comprehensive framework highlights the adaptability and inclusivity of governance mechanisms in fostering resilience and collaboration amidst evolving global health challenges.

As new threats emerge, diverse actions by global actors come into play. On one hand, new networks are established to address these threats, adapting to changing circumstances and vulnerabilities. On the other hand, existing networks expand, elevating the urgency and scope of security concerns to heightened levels. Concepts such as security governance, complex interdependence, and regimes play a crucial role in fostering critical thinking and advancing the analysis of international studies. These concepts are interconnected through the liberal institutionalism theory, which facilitates the inclusion of nonstate actors in networks by emphasizing trust, institutional legitimacy, and a high degree of institutional capacity (Pierre and Peters 2005). As a reinforcing mechanism, security governance provides a framework for addressing global security practices, regimes establish the *rules of the game*, and complex interdependence highlights the participation of diverse actors through multiple channels. However, the interconnected nature of these systems also introduces vulnerabilities and risks. While some scholars, such as Robert Keohane and Stephen Krasner, highlight the benefits of regime-building through interdependence, they also caution that competing interests and mistrust among actors can undermine regime stability (Keohane 1984; Krasner 1983). These dynamics emphasize the delicate balance between fostering collaboration and managing the tensions that arise within complex and interconnected systems of governance.

According to the United Nations (UN) high-level digital interdependence declaration on digital cooperation, “our aspirations and vulnerabilities are deeply interconnected and interdependent” (United Nations 2019a). The challenges of fostering international cooperation on issues like climate change and pollution often stem from political priorities, conflicting agendas, and the difficulty of aligning global commitments. Similarly, while responses to pandemics frequently emphasized national policies, the interconnected nature of infectious disease management underscores the necessity of collaborative frameworks. Nation-states, institutions, and nonstate actors play complementary roles in developing mechanisms that enhance global preparedness and capacity to address health crises. This perspective highlights the evolving dynamics of global governance, where collective efforts are essential in tackling shared threats.

Three additional areas of review–the sociology of health and technology, international law and policy, and intelligence studies–expand the theoretical foundation of this research. The sociology of technology explores the role of nonhuman contributors, such as codes, algorithms, and artificial intelligence, in shaping global surveillance networks. These technological components facilitate collaboration by building trust, achieving institutional acceptance, and fostering interconnectedness in addressing shared challenges. Similarly, international law and policy provide the regulatory frameworks that harmonize efforts among diverse actors combating infectious diseases. While intelligence studies traditionally focus on security threats, their inclusion in this context reduces uncertainty by leveraging data analysis and information sharing. These interdisciplinary insights collectively strengthen governance mechanisms and emphasize the necessity of collaboration in addressing complex global health challenges.

Interdisciplinary knowledge transcends traditional disciplinary boundaries, creating a cohesive framework for addressing complex global health and security challenges. The intersection of cybersecurity and global health becomes particularly significant as actors rely on secure, transparent data systems to manage public health crises. As nontraditional threats evolve, these networks bring together actors from various dimensions–nation-states, institutions, private industries, and nonhuman contributors such as technology platforms–to address shared concerns effectively. The interconnected nature of the digital ecosystem, while fostering global collaboration, necessitates vigilance to ensure that sensitive information remains secure and contributes positively to public health outcomes.

Balancing these risks with the benefits of enhanced surveillance and intelligence sharing remains a critical task for governance frameworks addressing AMR and emerging infectious diseases.

In conclusion, interdisciplinary knowledge unifies diverse theoretical frameworks to address the complexities of global health and cybersecurity challenges. Collaborative networks, supported by diverse theories and concepts, facilitate innovation and adaptability in responding to infectious diseases. As nontraditional threats evolve, these networks bring together actors from various dimensions–nation-states, institutions, private industries, and nonhuman contributors such as technology platforms–to address shared concerns effectively. However, sustaining such collaboration requires a system of robust governance rules, fostering trust and resilience among actors. This study acknowledges the ever-changing nature of global threats, emphasizing the importance of adaptive frameworks to safeguard against pandemics and other crises that disrupt global systems.

Structure of the Book

This book is organized into five chapters, starting with an introduction that outlines the research, the unit of analysis, and the justification for the study. It sets the stage by presenting the objectives, core research question, hypothesis, and the book's overall structure. Each chapter builds upon the previous one, offering a comprehensive exploration of global interconnectedness and security governance in the context of infectious diseases.

Chapter 1 explores the theoretical framework by examining three foundational theories and integrating insights from disciplines such as health, sociology, law, science and technology studies, and security studies (as detailed earlier). This chapter establishes a foundation for understanding the emergence of a health regime through collaborative governance.

Chapter 2 explores the study's methodology, divided into three sections: the research design, methodological limitations, and the data collection process. The latter encompasses two phases: quantitative data structure and qualitative data structure.

Chapter 3 presents the case study in four sections. The first section focuses on data analysis and results, emphasizing a single case study. The second section investigates communicable diseases, highlighting the GLASS technology database and eight bacterial pathogens, alongside the novel threat of COVID-19. The third section examines security governance using a metrics framework derived from document analysis and semi-structured interviews. Finally, the fourth section explores the GLASS and AMR case study, addressing COVID-19 as a contextual research and as a reinforcement mechanism within the study. This chapter also introduces five dimensions of security governance, focusing on the alignment of data sharing to promote a health regime.

Chapter 4 analyzes the study's objectives: (1) to open the black box of a health regime, (2) to analyze security governance in the context of unconventional threats, and (3) to examine the alignment of managed big data sharing. This includes exploring risks, vulnerabilities, and resources in surveillance systems like GLASS to build a comprehensive health regime. Lastly, chapter 5 presents the conclusions, synthesizing the chapters to tie all components together. It establishes the research findings and substantiates their relevance to the central research question and overarching theme of global interconnectedness.

This book examines security governance, global interconnectedness, and actor collaboration, emphasizing the role of technology in infectious disease surveillance to promote a comprehensive health regime. The research analyzes data from the WHO's GLASS monitoring system using an explanatory sequential design model with mixed methods, incorporating quantitative and qualitative techniques. By employing macro- and meso-level analyses, the study explores diverse realms inhabited by network actors. Data collection focuses primarily on the United States, complemented by insights from countries in the global South and other relevant actors contributing to the promotion of a health regime.

This research also incorporates data from expert interviews affiliated with the research analysis unit. The investigation focuses on countries in the southern subcontinent of the Americas, serving as the context of contribution throughout the chapters. While not a controlled comparative study, the research evaluates the evolution of country participation and the involvement of diverse actors between 2015 and 2021.

The study identifies the theories and methods central to its framework, discussed in detail in the following chapter. It defines security governance of infectious diseases as the independent variable and the perception of nonconventional threats in the emergence of a health regime as the dependent variable. Intervening variables include the potential manipulation of human bias, algorithmic influence, restricted information flow, and delayed dissemination of critical data.

The study employs a mixed-methods approach, integrating quantitative and qualitative data structures to analyze the dynamics of security governance in infectious disease surveillance. The quantitative data structure includes four collaborative network paths (CNPs)–CNP A, B, C, and D–created for visualization using the Force Atlas algorithm layout in Gephi (Bastian, Heymann, and Jacomy 2009). This enables statistical analysis of linkages between nodes and edges. Meanwhile, the qualitative data structure emphasizes triangulation, combining interview data with insights from other sources. Chapter 3 analyzes data and results, utilizing a case study to illustrate how collaborative networks address infectious disease threats. Through both quantitative and qualitative findings, the chapter explores the role of AMR surveillance and security governance mechanisms in promoting a health regime. This approach highlights the significance of security threats from the perspective of interconnected actors, including institutions and nation-states, at both local and international levels.

The case study emphasizes the role of the IHR as a central regulatory framework connecting nation-states and institutions. Through this collaboration, security governance mechanisms facilitate open data sharing, ultimately promoting a health regime aimed at monitoring infectious diseases. This study establishes the causal relationship between security governance and the emergence of a health regime by analyzing submissions from GLASS-participating countries. These submissions reflect the extent of collaboration within the surveillance network and the level of commitment from actors involved. Furthermore, the research addresses critical questions about the participation of GLASS member states, the role of AMR in health policy priorities, and the contributions of various actors in promoting a health regime through data sharing.

Pandemics often prompt centralized actions by nation-states, which subsequently decentralize through collaboration with entities like the WHO. These agreements drive collective responses to global health emergencies, such as combating bacterial pathogens. At the meso level, actors such as NGOs, academics, scientists, intelligence personnel, and security experts contribute to global public health within the network sphere. These actors collectively establish rules to address health and security threats. Conversely, the absence of collaboration fosters confusion, disinformation, and diminished legitimacy. Therefore, actors with shared interests in national security and civil society form a critical backbone of network collaboration.

This study also examines indirect relationships within the network, emphasizing the importance of identifying dissimilarities among actors. While some actors disrupt collaborative efforts, these disruptions can drive innovation and highlight the value of diverse interconnections. Ultimately, such disruptions challenge the network to foster improved collaboration and strengthen global interconnectedness.

In complex organizational settings responding to precarious situations, the question arises: Are we truly disconnected, or can actors–from nation-states to institutions–find ways to collaborate toward shared objectives? Recent experiences highlight the varied responses of organizations to threatening events. Are current preparedness measures sufficient for confronting unprecedented pandemics, or should AMR be considered the next silent pandemic? As this analysis unfolds, it is vital to recognize that the realities depicted here may quickly evolve. Data continues to proliferate, and infectious diseases propagate at astonishing speeds. The dynamic nature of global health challenges underscores the need for adaptability, resilience, and constant vigilance.

Actors exist within a web of interconnection, deeply intertwined with other actors and their environments. Global collaboration flourishes when shared interests and objectives align. Network analysis reveals the intricate structures formed by interconnected actors, both human and nonhuman.

By enabling the emergence of a security regime within a health regime, these collaborations bolster national security, enhance informed decision-making, and drive regional and global actions. However, interdependence also highlights the complexities and vulnerabilities of these networks, necessitating constant evaluation and reinforcement.

It is imperative to understand the role of actors within the international system, particularly those who disrupt collaborative efforts. Panic and uncertainty often spread faster than the threats themselves, amplifying the challenges of effective governance. A thorough analysis of network actors –including those withholding information, spreading misinformation, or engaging in disruptive cyber activities–provides insights into the limitations of global collaboration. Addressing these challenges requires proactive measures to foster interconnection and coordination among diverse actors, ensuring the resilience and effectiveness of governance frameworks.

- Our economy is intricately interconnected.
- Global health and well-being are fundamentally linked.
- Civil society relies on robust interconnectivity.

Global pandemics disregard national borders, highlighting the necessity of collective well-being and the challenges inherent in interdependence. The availability of data through an expansive information ecosystem enhances opportunities for collaboration and innovation. Economic stability relies on public health, just as health is deeply connected to security. These domains –economics, health, and security–are mutually reinforcing, creating a cycle that demands collaborative efforts to address nontraditional threats. Actors globally interconnect in a complex, interdependent world. This collaboration integrates human and nonhuman actors to address challenges such as AMR and COVID-19, strengthening global preparedness and resilience.

This introductory chapter has laid the groundwork for understanding the interconnections among various actors within a collaborative environment aimed at addressing the challenges to global health and security, particularly in relation to infectious diseases. It has provided a concise overview of the research study, including its justification, objectives, theoretical framework, and overall structure. The subsequent chapters of this book build upon the foundation established in this introductory chapter, delving into in-depth quantitative and qualitative data analysis to address the central research question. Through this exploration, the study aims to provide a comprehensive understanding of the dynamics among diverse actors and their roles in addressing the interconnected challenges of infectious disease surveillance, global health, and cybersecurity.

Chapter 1
Theoretical Framework

Sometimes all it takes, to crack a problem, is a new perspective.

—Adrian Tchaikovsky

Derived from the Latin term *ingentis*, meaning immense or vast, *ingentis data* is employed in this study to describe what is commonly known as big data. Defined by scholars as large datasets that exceed "conventional computational storage and analysis" capabilities, big data extends beyond sheer volume to include the digital traces of habitual activities (Halford and Savage 2017, 1133). The exponential growth of such data, coupled with escalating global security threats like infectious diseases, highlights the urgent need for enhanced security and privacy protection measures.

Actors in data sharing exchange critical information to address diverse interests. However, data sharing also introduces risks, as it can become a source of nonconventional threats when exploited by actors with access to open-source information. For instance, publicly available data on infectious diseases, such as pathogen genomes, transmission patterns, or healthcare vulnerabilities, could be weaponized by malicious actors. These actors might leverage such data to engineer more resilient biological agents, target critical healthcare infrastructure through cyberattacks, or manipulate emerging technologies to spread misinformation during crises.

By analyzing such risks, this chapter builds on existing literature to contextualize the study's findings, establish a foundation of knowledge, and identify prior scholarship. The central research question is as follows: Why did security governance, through the OSINT technology database of the WHO, promote the health regime on the surveillance of communicable diseases in the Americas from 2015 to 2021? The study focuses on this timeframe because significant events related to communicable diseases occurred during this period, providing a critical context for exploring the dynamics of security governance and its role in advancing global health efforts.

Which theoretical and conceptual framework aligns with the research question? This study adopts an approach grounded in liberal institutionalism theory, which, in international relations, emphasizes the importance of collaboration among states, institutions, and nonstate actors to address global challenges. Departing from the realist perspective that considers nation-states as the sole significant actors, this framework highlights the interdependence of various actors and the institutional arrangements that facilitate cooperation in addressing shared threats. By focusing on the interplay between state and nonstate actors, this study demonstrates the need for adaptive governance mechanisms to navigate the complexities of interconnected global systems effectively. This approach is supported by established scholarship that recognizes the value of institutional collaboration in managing transnational challenges (Keohane and Nye 1977; Krasner 1983). This approach highlights the adaptability in managed shared global challenges.

The analytical framework of this study integrates three key theories: liberal institutionalism, securitization, and ANT. Grounded in the concepts of complex interdependence, regimes, and security governance, these theories collectively provide a cohesive foundation for analyzing global health challenges. Liberal institutionalism, as explored by Keohane and Nye (1977), emphasizes the importance of collaboration among states and institutions in addressing shared challenges. Securitization theory, introduced by Buzan, Waever, and de Wilde (1998), analyzes how global health crises are framed as security concerns through social interactions among diverse actors. The ANT, developed by Latour and Callon, examines the interplay between human and nonhuman actors in collaborative networks, shedding light on mechanisms of translation and network stability essential to governance systems. This interdisciplinary framework enhances the study's capacity to address the complexities of infectious disease surveillance while fostering adaptability and inclusivity among diverse actors.

This study leverages and combines these theories and concepts to reinforce its examination and address three core objectives, abridged here from their comprehensive presentation in the Introduction chapter:

- To open the black box of a health regime by establishing the existence of a surveillance system for open data collection. This objective examines the strengths and weaknesses of policy instruments in national security, addressing issues such as the misuse of infectious diseases as biological weapons, cybersecurity vulnerabilities, and the impact of emerging technologies.
- To analyze how unconventional threats activate security governance, facilitated by international collaboration, *dispositifs*, and *boundary objects*. Using the GLASS as a case study, the objective highlights how open data exchange promotes a health regime for monitoring microbial pathogens that infect human beings.
- To explain why security governance effectively secures a health regime for infectious disease surveillance through OSINT. This objective identifies risks, vulnerabilities, and resources emerging from the interconnected nature of multiple actors during open data exchange.

This book is not limited to theoretical reflections alone, such as analyzing historical processes through actors' path dependence. Instead, it adopts a deductive model of explanation, using data from the United States and its interconnected actors to map the collaborative surveillance network of infectious diseases. This approach examines actor performance and interconnectedness, contributing to fields such as international studies, international relations, and science and technology. By focusing on institutions, regulatory operations, and technological advancements, the study explores how these elements interact within the network of global health governance.

The research acknowledges the importance of boundary objects, such as GLASS and the IHR, which facilitate collaboration and bridge disciplinary divides. These objects have emerged through the efforts of actors from diverse professional and scientific backgrounds. While boundary objects enable collaboration, challenges may arise due to differences in expertise, technical systems, and practices. This study highlights the role of these boundary objects in addressing security threats, emphasizing their relevance at both international and local levels.

This study highlights how GLASS, as a nonhuman actor, plays a central role in the interconnected paradigm of global health governance. The IHR, as a governance instrument, sets the rules for participating countries, shaping the collaborative processes within the network. Additionally, interactions among actors–including ideas, discussions, and preparedness efforts–strengthen the capacity to address microbial threats (Pestre 2012). Thus, the IHR, GLASS, and infectious diseases function as boundary objects that link communities and fosters interconnectedness.

Which theoretical perspectives explain how social change has shaped international responses to health, security, and interconnectedness? Three theoretical perspectives address the central research question. Liberal institutionalism theory positions states as one of many significant actors, emphasizing cooperation within the international system. ANT complements this by uncovering the network's limitations and exploring the relational ties between human and nonhuman actors. Technologies often act as the *glue* binding actors within this complex interdependent framework. Additionally, securitization theory interprets how groups construct issues as security threats, functioning as a causal mechanism that evolves to address multifaceted challenges over time.

Likewise, which concepts emerge as integral to addressing the research question of health and security? This study examines three core conceptual processes: the complex interdependence of actors at the global level, the establishment of a health regime encompassing regulatory and security measures, and the security governance of the disease and the data (including the management, control, and risk). Through the GLASS case study, this research illustrates how international collaboration, the IHR, and global surveillance systems collectively shape governance structures that respond to health crises effectively.

Traditionally, the state–particularly through its military apparatus–played a dominant role in the international system. However, the concept of complex interdependence has expanded the avenues for global actors to connect through multiple channels. This dimension allows for deeper exploration of collaborative mechanisms. Regimes establish the *rules of the game*, fostering interdependence among actors. This study demonstrates that the IHR, a boundary object functioning as an instrument of governance, law, and policy, sets the standards for promoting a health regime. Similarly, security governance structures the responses of interconnected actors to address security threats effectively.

In addition, interconnectedness is facilitated through channels such as transportation and the internet, which enable collaborative interactions that promote stability and preparedness. By adhering to regulations and engaging in collaboration, actors create order rather than chaos. As Knoke (1993, 170) aptly observed, "Collaboration among actors who pool their power resources is generally more effective in realizing their common interests than are efforts by actors attempting influence and domination on their own." In addressing public health issues, actors prioritize managing global health through the integration of data, statistics, and incident analysis, which collectively shape security, health security, and trade security (Quet 2022). This study highlights how human actors collaborate by inputting data into publicly available surveillance technology databases (nonhuman actors), driving the phases of security governance.

Multidimensional regimes encompass a range of elements, including cooperation and collaboration, which are pivotal to the security sector. While decision-makers often prioritize competitive strategies to align with their interests (Jervis 1982), the 1980s marked a shift toward international collaboration as a prominent form of engagement, emphasizing mutual benefit over technical assistance (Gaillard and Arvanitis 2014). This study foregrounds the critical role of collaboration as a dimension integral to addressing global challenges.

Adopting a perspective that transcends a state-centric view, as Holsti (1986) suggests, enables a broader understanding of international collaboration and its influence on global affairs. Regimes serve as active frameworks that guide individual decision-making processes (Krasner 1982). Norms explain the motivations behind state collaboration, rules define the purpose of these interactions, and procedures delineate the mechanisms for achieving collaboration (Haas 1980). Together, these elements foster a structured and systematic approach to global cooperation.

The increasing complexity of technology has catalyzed collaborative efforts among actors in science and technology (Arvanitis 2009). These collaborations occur at multiple levels: the national and institutional levels, where efforts are driven by national security and societal concerns, and the international level, where global networks address issues such as health and infectious diseases. Gaillard and Arvanitis (2014) identify three tiers of collaboration: the policy environment and instruments shaping collaborative decision-making, the international level encompassing global networks tackling issues such as global health and infectious diseases, and the individual level where personal choices, disciplinary affiliations, and career trajectories influence collaboration. These dimensions of collaboration resonate with the research's central theme and vision, illustrating the multifaceted nature of addressing global challenges.

Interconnection refers to the links between actors within a network, which are vital to the effectiveness of an institution's strategies and ideas. Strong interconnections amplify collaboration among actors, facilitating the achievement of shared objectives. These connections include both strong and weak ties, reflecting varying levels of influence and interaction. For instance, during health crises, interconnection issues, such as misinformation, inadequate communication, and disparities in healthcare access, can exacerbate challenges. Such issues underscore the importance of understanding the relationship between nations with high contagion rates and those experiencing elevated mortality rates.

Interconnection also manifests in decision-making processes within institutions like hospitals, where groups oversee the selection of tools for production, data sharing, and monitoring. However, the absence of clear governance structures hampers negotiations and mediations, obstructing the achievement of network goals. The COVID-19 pandemic illustrated these challenges, as inconsistent coordination between local and federal governments destabilized efforts to manage the crisis effectively. This lack of alignment highlights the critical need for clear rules and robust frameworks to support collaborative efforts during global emergencies.

In some instances, actors discreetly organize collective reflection across diverse institutions, drawing on expertise from disciplines such as medicine, law, economics, and political science (Boudia 2014). Such collaboration led to the creation of the Committee on Institutional Means for Assessment of Risks to Public Health, commonly referred to as the *Red Book* of risk assessment. This report identified priority areas, including health, air transport, and nuclear energy, where research would refine analytical methods (Boudia 2014). These initiatives demonstrate the value of social control mechanisms and structured systems of rules within collaborative networks. By uniting actors under a shared purpose, these mechanisms significantly enhance the capacity to achieve collective objectives.

In today's complex world, entities confront unconventional threats like infectious diseases, which challenge traditional notions of security. Objectively, security measures aim to eliminate threats, protecting core values, while subjectively, they seek to alleviate fear arising from perceived vulnerabilities (Saint-Pierre 2017). Heightened threats elevate health security concerns for both state and civil society actors, driving collaborative responses. The theories underpinning this research form the skeleton of the chapter outlines, providing structural support, while the concepts serve as the heart and brain of the study, driving its intellectual and analytical core. Together, they interconnect, like muscles, to articulate how perceptions of nontraditional security threats contribute to the emergence of a health regime.

The Evolution of Theories

The theoretical framework builds on three theories: the liberal institutionalism theory using a case study, the securitization theory using context analysis, and the actor-network theory using network analysis. These theories intertwine to explain the phenomenon of a health regime. How does open data through a surveillance system of infectious diseases pan out with respect to security measures? Thoughts of battling other sources of nontraditional threats emerge, such as attacks using biological weapons, cybersecurity, and emerging technologies. The phenomenon exists independent of social actors, guiding the researcher's ontological and epistemological position and choice of methods (Fontaine 2015; Grix 2002), while positivism advocates applying natural science methods to studying social reality (Grix 2002). This study adopts a positivist approach and uses an objective ontology, treating international regimes as structured entities that guide actor behavior and influence decision-making. For example, Krasner (1982) examines how regimes establish norms and rules to shape interactions among actors, while Keohane and Nye (2012) highlight their functional role in facilitating cooperation in a complex, interdependent world. Additionally, Pestre (2012) emphasizes the importance of knowledge production within institutional contexts, complementing this perspective by illustrating how norms and standards are defined to address global challenges. Incorporating these perspectives enriches the analysis by offering a multidimensional understanding of the emergence and governance of a health regime, highlighting both the structural and dynamic processes that drive global cooperation.

To comprehend the articulation of norms by actors, it is essential to identify the key participants in the transformation process, understand their interactions, and assess their influence on security. The creation and dissemination of facts increasingly involve nonhuman actors alongside human agents. The presence of *ingentis* data within a data framework such as GLASS integrate vast datasets, which shape decision-making processes in infectious disease surveillance. However, this research acknowledges that these nonhuman entities operate interdependently with human actors. Theoretical, ontological, and epistemological foundations thus provide a robust basis for assessing these interactions and anticipating developments to enhance a health regime.

The theories collectively provide tools to unpack the complexity of the *black box* of a health regime (Latour 1987). This conceptual black box houses various interconnected and collaborative actors. For example, nonhuman actors, such as the IHR and GLASS, play pivotal roles in security governance of infectious diseases beyond national borders by standardizing global responses to health threats, facilitating cross-border data sharing, enhancing surveillance capabilities, and ensuring coordinated responses to infectious diseases. These frameworks provide structured mechanisms that guide collaborative efforts across nations, thereby addressing health threats beyond national borders. By incorporating human and nonhuman elements, the theoretical framework facilitates a comprehensive understanding of these dynamics, providing insights into the mechanisms of collaboration and resilience within health regimes. Thus, independent of social, network, and structural actors, the phenomenon opens the door to analyzing risks and vulnerabilities.

Liberal Institutionalism Theory: Enabler of Action in the Sea of Global Complexity

The changing balance of power from military capacity to economic status within a specific sector (health care) highlights the necessity for stronger connections and enhanced collaboration. In the field of international studies, liberal institutionalism emerges as a primary approach, enabling various theories to converge by virtue of shared mechanisms for analyzing the international system. The emergence of technological advancements, previously considered peripheral and contrary to realist perspectives, now gathers momentum due to increased global interconnectedness. Should we consider it wiser to initially break down and examine the terminologies individually before delving into the actual theory?

Liberalism (Kant 2006; Smith 2000; Locke 1980) speaks of the role of institutions, norms, the impact of state behavior, and the implications of interdependence. Liberalism examines state actions and directs its attention to other groups (Keohane and Nye 2012). Intergovernmental actors such as the United Nations are essential in international relations (Abbott and Snidal 1998). International organizations "facilitate the diffusion of world culture" (Chorev 2012, 18). For example, in 2002, an international institution, the World Bank, delivered learning activities to over 48,000 participants in 150 countries through collaboration with more than 400 institutions to develop knowledge networks in the field of economic development (Goldman 2005). The liberal or Grotian tradition stresses the effect of complex interdependence, international society, and international institutions (Keohane and Nye 2012). Liberalism associates itself with a more liberal theory of regimes that help states realize common interests, and state actions depend on prevailing institutional arrangements (Keohane 1984). Thus, liberalists seek interdependence to analyze issues such as the transfer of technology (Viotti and Kauppi 2012) as an opportunity for building good relations between interdependent units because institutions affect global issues and relations of actors on the world stage.

Institutionalism emphasizes the significance of international organizations as pivotal players in global politics, where diverse actors collaborate to address shared challenges. These institutions co-produce global frameworks (Jasanoff 2004) and legislate interests, conflicts, and values (Pestre 2012). For instance, intergovernmental organizations like the United Nations Security Council and the WHO manage interstate relations to tackle contemporary security threats, including global health crises (Krahmann 2005; Abbott and Snidal 1998). Their independence, centralization, and unique activities position them as crucial actors in global security governance (Arvanitis 2009; Abbott and Snidal 1998). Normative frameworks established by these institutions strengthen collaborative efforts by prescribing behaviors aligned with collective goals, such as advancing global health (Keohane and Nye 2012; Viotti and Kauppi 2020). Within this context, the WHO exemplifies how complex interdependence fosters collaboration among state and nonstate actors to safeguard *ingentis* data, combat nontraditional threats, and promote global health. By increasing interdependence, these institutions enhance global security and their role becomes indispensable in addressing multifaceted global challenges (Keohane and Nye 2012). By bridging these interdependencies, institutions play a critical role in fostering resilience and coordinated responses to shared global challenges.

The liberal institutionalism theory represents advancements in the interconnectedness between states and institutions. It provides an understanding of the dynamics of international cooperation amongst actors (Abbott and Snidal 1998; Keohane 1988, 1989). Under liberal institutionalism, the states maintain a primary role but are not the only significant actors in international relations. The process of elaborating norms coincides with implementing new norms where "the state is no longer the monopolistic provider of the means of enforcement" (Brousseau, Marzouki, and Méadel 2012, 5). Other actors, such as international organizations, NGOs, and private interest groups (foundations and companies), also exist in an area traditionally reserved for the state. Some notable scholars emphasize institutional details through their increased role in peacebuilding (Cox and Jacobson 1973; Kirchner and Sperling 2007). At the same time, others analyze institutions through their transformational effect on decision-making (Fontaine 2015; Pierre and Peters 2005). Likewise, the theory emphasizes intergovernmental affairs, such that regimes help actors reach collaborative agreements (Abbott and Snidal 1998; Keohane 1984). This study shows that an institution creates a surveillance system database in which various participating countries gain access and collaborate in monitoring bacterial pathogens that affect human beings and also AMR. However, is data sharing getting into the wrong hands and generating unwelcome actions of nonconventional threats? Thus, a progressive theory of liberal institutionalism drives this investigation to unravel the question.

Indistinguishably, literature shows countering arguments between realists and liberal institutionalists. For instance, international organizations have unstructured internal management of international agencies and need help to solve external issues (Claude 1971). In addition, international organizations need more of a voice in their agenda to disseminate information (Chorev 2012). Similarly, the WHO remains dependent on international funding by philanthropic organizations and establishes policies managed by large NGOs. Grieco (1988) notes that states are the primary actors in global affairs and that joint gains produce potential foes in the future. Likewise, institutions exist not in high-level sectors such as national security and defense politics but in low-level sectors such as health and communication (Mearsheimer 1994). Lakoff (2017) discusses how nation-states remain the source of authority.

Additionally, in the twenty-first century, the WHO acts as an administrative coordinator and technical norm-maker, and the ability of the IHR framework "to govern the actions of states in the name of a global space of public health security was highly constrained" (Lakoff 2017, 3). Hoffman (1995) questions the United Nations' capability during the Cold War. The author's stance on institutions during the Cold War indicates that international organizations paralyze the economic needs of liberal states when tackling security issues. Therefore, scholars argue that institutions carry little weight in dealing with world affairs.

Nevertheless, nonstate actors, such as institutions, nongovernmental organizations, and private interest groups (philanthropic and foundations), play a significant role in the network dichotomy. Here, the WHO developed a surveillance system against AMR. The GLASS created a platform where participating countries voluntarily enroll and input information from their respective countries into this openly available database. As one of the power players in the collaborative network, the institution creates a system to link the actors. Therefore, due to increased interdependence, nontraditional actors play a significant role in global governance.

Likewise, a global health regime serves as an institution. Keohane (1988) indicates that examples of institutions include the UN and the World Bank. Institutions refer to a general pattern of activity and a complex set of rules and norms identified by time and space (Stein 2008; Keohane 1988). General patterns of international society characterize institutions (Bull 1977) and varied behavior patterns (Keohane 1988; Young 1982). Coincidently, these definitions mirror regimes (Krasner 1982; Puchala and Hopkins 1982; Jervis 1982). For example, the WHO's pattern of activity enforces global health in the interest of civil society and the state. However, Lachenal (2013) illustrates how social actors need to emphasize the relationship between the prevention and cure of diseases to fit specific organizational needs due to their way of acting internationally. Through document analysis, this study shows questionable aspects of collaboration among the participating countries. Various intermediate actors such as NGOs, private interest groups, and medical teams influence the international system of global health and collaborative network.

In 2014, the WHO published a report assessing the extent of AMR and the state of global surveillance at that time (World Health Organization 2014). From 2015 onwards, the WHO has consistently issued reports in collaboration with various centers and partnerships as well as organized events focused on AMR. These initiatives demonstrate a consistent pattern of behavior aimed at supporting the action plan on AMR and fostering global data sharing. However, how influential are institutional actions on global health and security when a push for global health investment exists and its framing has to consider citizens and the nation's security? Chorev (2012) notes that the WHO only generates revenue with resources and international funding from voluntary donors, participating countries, and philanthropic organizations. Examples of these organizations include the Rockefeller Foundation, the Bill & Melinda Gates Foundation, and the Wellcome Trust. In 2017, large parts of the funding focused on the African region (21.7%) and the Southeast Asian region (57.1%), where most outbreaks and emergencies appear (World Health Organization 2018d). As of December 31, 2018, the WHO reported a total of $723 million in available funds and $38 million toward AMR (World Health Organization 2018d). However, the global South received the least amount of funding ($20 million) compared to Africa ($193 million) and Southeast Asia ($99 million) owing to a high level of emergency, which illustrates an uneven distribution (World Health Organization 2018d). Thus, voluntary contributions influence the spending of funds.

In 2019, the WHO welcomed new funding commitments at the Global Fund's Sixth Replenishment Conference to finance the fight against infectious diseases (World Health Organization 2019c). At the same time, Wellcome Trust tackles drug-resistant infections and advances global surveillance of communicable diseases (World Health Organization 2019c). However, would the actor's actions also influence and change the way institutions and countries consider a national security threat?

Institutions provide a "higher power in shaping situations" (Pestre 2012, 437). Technological advancements are accelerating global transformations, which in turn give rise to new security threats. It is a complex reality that data grow exponentially, and that diseases spread like waves in an ocean, manifesting many global changes. Policies, laws, and diverse forces interconnect in tackling issues to meet new movements and expansion. The history of the Cold War sets a precedent for change. Prior experiences in international relations opened the door to exploration of advocating norms and values in global movements. Threats will continue in the future and tackling them will need an all-hands-on-deck approach. Thus, institutions and many other actors tackle new threats by adopting a more liberal institutionalist and progressive approach to network collaboration.

Securitization Theory: What is a Threat? In the Eyes of the Beholder or None

Security of one person is not a security threat to another. Similarly, nation-states have different values, practices, and considerations in defining a threat. How do actors interpret security, and what instruments facilitate the process of interpretation? The securitization theory provides theoretical lenses to explain and understand what security for different actors entails. Constructivism originates from sociologizing security analysis. However, a more objectivist progressive approach uses securitization as a causal mechanism of a particular outcome. Scholars understand security through its performance, otherwise known as securitization. Securitization has multiple analytical dimensions and a lifetime career. Securitization acts as a framework of analysis, empirical theory, and conceptual move (Guzzini 2011; Kirchner and Sperling 2007). It opens the possibility of thinking about security on different issues. This research analytically draws toward a progressive viewpoint and designates referent objects. Likewise, securitization theory functions as a causal mechanism to explain the emergence of a health regime. It serves as an entry point into the rich empirical world to comprehend the extent to which states and institutions respond to health threats and technological advancements. Under the securitization theory, actors handle security issues urgently due to their heightened, menacing, and threatening level when labeled as dangerous political issues (Eroukhmanoff 2017; Kirchner and Sperling 2007). Thus, an existential threat presents an unprecedented response.

In addition, the securitization theory links liberal institutionalism and ANT by connecting external effects in the world. Traditionally, the safety of the state remained a priority for security. However, in showing more actor-action-oriented mechanisms, a level of causality appears that turns the attention toward *referent objects* (Eroukhmanoff 2017; Kirchner and Sperling 2007) raised as security matters on the agenda.

Referent objects of security include threats to cyberspace and to citizens' health and wellness in combating infectious diseases and the misuse of massive amounts of data.

According to the Copenhagen school (McSweeney 1996), the traditional meaning of securitization refers to security posing as an existential threat "understood as an essentially intersubjective process" (Buzan, Waever, and de Wilde 1998, 30). The threat rises to a level of urgency when securitizing actors break from the normal agenda they would otherwise be bound by (Buzan, Waever, and de Wilde 1998). This analytical knowledge level reinforces the state's causal theory, institutional behavior, and context for qualitative data analysis. Scientific studies examine issues based on considerations "in accordance with institutional situations, depending on where the knowledge is produced" (Pestre 2012, 427). By contrast, limitations stem from the asymmetric interests of varying countries in the securitization of infectious diseases (Jin and Karackattu 2011).

Nonetheless, securitizing actors look to extreme alert status to escalate the security issue on the agenda (Šulovic 2010). While securitization cannot be a forced idea, successful securitization depends on the audience for security speech (Buzan, Waever, and de Wilde 1998), which reinforces its existential threat. For Eroukhmanoff (2017, 104), a securitizing actor "has the social and institutional power to move the issue beyond politics." Securitization focuses more on referent objects (Eroukhmanoff 2017; Kirchner and Sperling 2007). A community looks to a matter as an existential threat to a referent object of such high risk that it rises to the level of urgency and needs exceptional measures to handle the threat (Guzzini 2011; Buzan and Waever 2003). Assessment tools (such as the cost-benefit of developing and participating in the GLASS database) make it conceivable to address risks that present threats (Beck 1992; Pestre 2012). Likewise, securitization allows an assemblage of practices contextually mobilized by a securitizing actor to explain a referent object (Balzacq 2011). Thus, referent objects of security remain with citizens' health and wellness in combating infectious diseases, the misuse of big data, and threats to cyberspace information.

Distinguishably, Wolfers indicates that in an objective sense, security "measures the absence of threats to acquired values" (Wolfers 1962, 150). Likewise, Buzan, Waever, and de Wilde express leniency toward an objectivist approach when the "threat is unambiguous and immediate" (Buzan, Waever, and de Wilde 1998, 30). Some authors express dissatisfaction with the Copenhagen school's limitation of securitization by not addressing causality and indicate that the securitization process introduces a more progressive positivist stance and analyzes a causal mechanism (Oliveira 2017; Balzacq 2011; Guzzini 2011). Moreover, rationalists use a middle-ground approach to broaden securitization status and define it as a *causal complex* (Oliveira 2017). Other authors stress that the "task of a sociological theory of securitization . . . is to decipher the sequences of cause-and-effect" to stand "at the center of its explanatory architecture" (Balzacq 2015, 110). Securitization is both *explanandum* and *explanans*, seen as a process that triggers certain effects (Guzzini 2011). From Wolfers's (1962) objective security stance to Buzan, Waever, and de Wilde's (1998) indicating an immediate and unambiguous threat as an objective approach, the doors of securitization open to include quantitative analysis. Therefore, securitization serves as a causal mechanism in the surveillance of infectious diseases and the emergence of a health regime.

Furthermore, the securitization theory opens the window of discourse in understanding how political actors address the link between cyberspace and national security because the securitization process involves multiple settings and political functions (Balzacq and Cavelty 2016; Guzzini 2011). The rise of strains of pathogens resistant to certain drugs influenced the launch of the Global Health Security Agenda (GHSA) in 2014. By 2015, the WHO developed the GLASS, asking participating countries to contribute and share their respective information on the surveillance of infectious diseases. Does contributing knowledge through open-source intelligence present a level of insecurity?

The presence of infectious diseases, big data, and advanced technologies brings about significant consequences. In this context, the existence of computer networks introduces a potential realm for cybersecurity.

According to the data from 2016, the top ten countries with the highest percentage of machine attacks and the greatest likelihood of new threats were El Salvador (10.85%), Brazil (10.04%), Bangladesh (9.77%), Honduras (9.44%), Russia (8.96%), Venezuela (8.87%), Colombia (8.29%), Pakistan (8.17%), Mexico (7.99%), and Ecuador (7.67%) (Panda Security 2017; Balzacq and Cavelty 2016). In contrast, the United States had the lowest infection rate, with less than 2% in 2016 (Panda Security 2017). These findings highlight the risks faced by countries in terms of cyberattacks, particularly in data sharing and exchange of information, which continue to grow with technological advancements. According to the Cybersecurity and Infrastructure Security Agency (CISA), malware attacks or malicious software have the capability to compromise a system by executing unauthorized functions or processes. Malicious cyber actors utilize malware as a means to surreptitiously compromise and gain access to a computer (CISA and ACSC 2022). Common types of malware strains include Remote Access Trojans (RATs), banking Trojans, information stealers, and ransomware. In 2021, the top malware strains identified were Agent Tesla, AZORult, Formbook, Ursnif, LokiBot, MOUSEISLAND, NanoCore, Qakbot, Remcos, TrickBot, and GootLoader (CISA 2022).

In contrast, regarding infectious diseases within the health sector, the WHO reported that in 2015, an estimated 2.1 million people were newly infected with Human Immunodeficiency Virus (HIV) and 1.1 million people died of HIV-related illnesses (WHO 2017f). By the end of 2015, there were approximately 36.7 million people living with HIV (WHO 2017f). In 2016, the WHO reported that an estimated 1 million people died of HIV-related illnesses (WHO 2018c). Regarding malaria, the WHO estimated 212 million cases globally in 2015, resulting in approximately 429,000 deaths (WHO 2017f). By 2016, the number of malaria cases had risen to around 216 million, with approximately 445,000 deaths reported worldwide (WHO 2018c, 2017f). It is a matter of concern that malicious cyber actors exploit these escalating global health issues. For example, in 2021, cyber criminals carried out phishing campaigns utilizing malware such as Agent Tesla, Remcos, and

Formbook and employing COVID-19 pandemic-related themes to illicitly obtain data from individuals and organizations (CISA 2022).

The involvement of nonhuman actors, from infectious diseases to the use of malware by malicious actors, presents the challenge of finding a balance between health and security. The prevalence of infectious diseases, as well as the "desperate health conditions of the poor and other vulnerable populations across the globe" (Chorev 2012, 3), coupled with the devastating impact of the HIV/AIDS epidemic and international concerns over the Zika outbreak (Lakoff 2017), all contribute to the rise of modern-day nontraditional security threats. Cyberattacks compound these issues, exerting influence on this delicate equilibrium.

Once organizations establish protocols such as the IHR, actors utilize these instruments repeatedly. As an inscription device, the IHR is effective in converting facts into a regime of norms (Jasanoff 2004; Latour 1987). However, this leads to the following questions: If the context evolves, does the protocol remain unchanged? How can the IHR operate as *dispositifs* or devices that enable the transfer of inscriptions between actors, shaping the definition of reality in a specific manner?

The securitization theory offers a valuable framework for conducting a systemic review of the varied responses of participating countries to the surveillance of infectious diseases. By employing the lens of securitization, the interactions between state and nonstate actors can be effectively analyzed. Security governance plays a crucial role in understanding and elucidating the dynamics and interplay between these actors. In the context of promoting a health regime, a causal analysis of security governance considers the social reality and prioritizes preventive and containment measures for communicable diseases. The analysis takes into account the causal powers that interact with the complex web of causality shaping the global landscape (Oliveira 2017). According to Oliveira (2017), the complex interaction of four causal forces–formal, efficient, material, and final–helps explain change. These forces shed light on the intricate dynamics at play within security governance. The forthcoming chapters of this book delve into a detailed causal analysis of securitization, unraveling the multifaceted aspects of this phenomenon.

Actor-Network Theory: Imbroglios of Network Interactions from Health to Security

As a system of rules, security governance reinforces cybersecurity practices, which leads to effective interventions and collaboration by diverse actors to promote a health regime and tackle secondary threats such as cyberattacks. The actor-network theory originates from science and technology studies and enables us to analyze the network's limitations and incorporates the junction of two worlds, human and nonhuman actors, into the hybrid space of analysis, organizational techniques, interactions, and calculations (Latour 2005). Scholars such as Latour suggest that we live in the reality of a hybrid world of "gods, people, stars, electrons, nuclear plants, and markets" that either turn into shambles or an ordered world (Latour 1999, 16). How would ANT inspire this research to comprehend the network process? Five loops in an actor network[1] involved in policymaking unravel the mediations between political, legal, and collaborative networks, and ANT describes the process of five loops or heterogeneous elements woven together for a realistic rendering of science as instruments, colleagues, allies, the public, and knots (Latour 1999). The present study shows that the IHR provides the governing rules between actors in the network. These regulations implement change in the exchange of open data sharing in the surveillance of infectious diseases. The actor-network theory reties and crisscrosses the knot to allow deeper insights by incorporating the collected data. The imbroglios weave our worlds together into an intricate and perplexing phenomenon that intertwines different political hemispheres (Latour 1993). Thus, the social and the technical cannot float separately in an autonomous sphere but live collectively in an intertwined world.

An essential aspect of using ANT is its principle of radical symmetry, which acknowledges the agency of both human and nonhuman actors. Radical symmetry posits that the qualities and defects attributed to

---

1 The term actor network in science and technology studies (STS) proposes that actors approach any system by viewing all parts as active and interconnected members, with each component, such as nature, technology, and humans, considered equal parts of the system (Latour 1988; Callon, Law, and Rip 1986; Law 1984).

humans–such as rationality or irrationality–are equally distributed among nonhuman actors (Latour 1987). This principle helps dismantle traditional distinctions between humans as willful agents and nonhumans as passive objects, enabling a more inclusive understanding of actor-network compounds (Law 1992). In this context, an actor is not merely an individual entity but a network effect, emerging from a web of heterogeneous relationships (Latour 1987; Callon, Law, and Rip 1986). ANT's approach to symmetry reveals how human behaviors–such as thinking, producing, and reproducing–are co-constructed within these networks, which transcend the boundaries of the body (Latour 1987).

Applying this perspective to the research, AMR pathogens, microbes, and other nonhuman actors, traditionally seen as mere biological phenomena, emerge as active participants in shaping health outcomes and economic systems. These actors not only cause illnesses and deaths but also interrupt economic development. For instance, the behaviors of pathogens can change in response to human interventions, such as the overuse of antibiotics, which redefines their performance and role within the network. By treating society and nature symmetrically, ANT provides a framework for analyzing the interconnected relationships that drive global health challenges, shedding light on the co-evolution of human and nonhuman actors.

Moreover, ANT inscribes practices into our technologies, revitalizing the connection between material objects (nonhuman) and cultural practices (human) to ensure continuity across various cultures throughout time (Balzacq and Cavelty 2016; Latour 2005; Jasanoff 2004). No division exists between humans and nonhumans as the theory seeks to define the relational ties between such actors within a network with equal value (Balzacq and Cavelty 2016; Latour 2005; Star and Ruhleder 1996). Network analysis emphasizes social relationships that create structures among actors and allows for socialization and diffusion in international relations (Hafner-Burton, Kahler, and Montgomery 2009). Thus, technology advancements affect the international system since incentives influence culture, and ANT gains momentum in international relations.

Likewise, ANT captures the apparatus (*dispositif*) that facilitates the inscription and translation process through hybrids or networks of human and nonhuman actors to break into material and immaterial objects (Albornoz, Bustamante Salamanca, and Jiménez Becerra 2012; Callon, Law, and Rip 1986; Jasanoff 2004; Latour 2005). The *dispositif* refers to the apparatus or the nature of the connection between heterogeneous elements such as "discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions" (Foucault 1980, 194). Properties of institutions include a collective purpose and purposeful action (Latour 1999). Likewise, apparatuses are the properties of institutions (Foucault 1980). For example, the GLASS uses the WHONET database software to manage and analyze antimicrobial results, which can be exported to the GLASS data structure (World Health Organization 2017b). Therefore, the GLASS offers a global surveillance system to standardize the collection, analysis, and sharing of AMR data and uses the WHONET as a conditioning apparatus to transform data.

The WHO, through GLASS, its administrative mechanism or instrument (inscription device), produces inscriptions such as visual displays, layers, and associations (Latour 1999). For instance, the setup of visuals provides a final layer in scientific text. This study shows that the WHO and the GLASS ensure submission of AMR data directly from countries and established official AMR surveillance networks, specifically the Red Latinoamericana de Vigilancia de la Resistencia a los Antimicrobianos (Latin American Network for Antimicrobial Resistance Surveillance, ReLAVRA for its initials in Spanish), European Antimicrobial Resistance Surveillance Network (EARS-Net), and Central Asian and European Surveillance of Antimicrobial Resistance (CAESAR) (World Health Organization 2021d, 2017b). The WHO and GLASS connect with microbiologists, epidemiologists, and scientists to gather data on pathogens and AMR, the GLASS serving as an instrument of producing and sharing data. The system yields inscriptions that produce GLASS reports, GLASS enrollment maps, and graphs of country AMR surveillance for bacterial species. From the WHO the GLASS emerges as an instrument that member states and scientists (human actors) collect data on pathogens to create raw images (nonhuman actors) used in GLASS reports and the website. Thus, the interface results in the production of a hybrid mixture of human and nonhuman actors. Likewise, no matter how many participating member states enrolled and submitted AMR data to participate in the construction of the images or took such data from 2015 to 2019 (the early implementation phase) to harmonize global collaboration, the WHO-GLASS illustrates an instrument. Therefore, nonhuman actors, such as the IHR and GLASS, work as instruments to transmit meaning and to produce data and as instruments of data sharing, monitoring, governance, law, and policy.

Furthermore, another concept of science and technology studies (STS) is *boundary objects* (Star and Ruhleder 1996; Bowker and Star 1999; Star and Griesemer 1989), which does not derive from ANT but complements the ANT approach. Boundary objects stem from STS that distinguish and provide common reference points. They consist of objects such as the social world, negotiation processes, mediators between groups, information, organizational arrangements, or any concrete element that helps draw the boundary between data and policy (Orsini, Louafi, and Morin 2017; Star and Griesemer 1989; Gieryn 1983). A constructivist position notes boundary objects as synonymous with interpretive flexibility (Star 2010). An objectivist ontological position looks at boundary objects as an organizational structure or arrangements, through the object's granularity scale, which help actors collaborate for a common interest (Bowker 2001). Other ANT scholars note that objects (Bowker 2006; Callon, Law, and Rip 1986; Law and Singleton 2005; Mol and Law 1994) come in diverse forms influencing the international system. To understand the importance of technical objects within networks, we have to constantly move between the social and the technical and see the ability with which actants reshape the object (Akrich 1997). Once viewed from this perspective, the boundary between the inside and the outside of an object is a consequence of the interaction rather than something that determines it (Akrich 1997). For instance, objects address modern security threats, monitor cheating, and ensure compliance with the regime (Krahmann 2005; Stein 1982). Likewise, biosecurity is a boundary object representing heterogeneous security dynamics and is a response to the issues of securing life in the state, scientific, and social contexts (Samimian-Darash, Henner-Shapira, and Daviko 2016). Thus, anything is considered a boundary object in the eyes of the beholder.

This research draws upon data from the GLASS architecture, in which participating countries collaborate to report information arising from monitoring of AMR. Therefore, collaboration requires information exchange, a mediator between groups, and the GLASS represents a boundary object as a mediator, a bridge, and an information producer. Moreover, the GLASS network and its WHONET surveillance and data management software stand as boundary objects when they act as a mediator between groups and report on eight bacterial pathogens that infect humans. The objects push the boundaries of country collaboration and participation in the surveillance of infectious diseases. The information circulates within cyberspace and brings diverse groups of actors together, such as the national coordinating centers (NCC), national reference laboratories (NRL), surveillance and quality assessment collaborating centers, participating countries, decision-makers, scientists, and researchers. Cyberspace develops as a network of physical nodes of servers scattered worldwide (Carril 2020). It co-creates spaces because cyberspace includes *ingentis* data being exchanged and shared, raising cybersecurity issues. Thus, boundary objects allow a better understanding of the network's dimensions, which complements the ANT approach in human and nonhuman actor symmetry.

In conjunction, translation is a method where actors enroll others, which involves defining and distributing roles, the actor-world strategy with passage points, and the displacement other actors receive in following the script (Callon, Law, and Rip 1986). Institutions help to build an actor world, and ANT incorporates the translation process to explain the legal and technical constructions (Vinck 2010) with scientific and political sites (Balzacq and Cavelty 2016). The purification process establishes the limits between humans and nonhumans to translate the act of national security into truth (Latour 1993; Callon, Law, and Rip 1986). The purification process reveals the layers of a global threat in the form of a pathogen as a matter of interest to national security. However, do boundary objects need to be more effective when the translation fails? This study shows that the WHO translates communicable diseases by generating awareness and support for the participating countries through its GLASS and draws maps and an indeterminate number of translations (Star and Griesemer 1989), and the IHR set the game's rules and generate a compendium of boundary objects. The WHO-GLASS translates into a boundary object as a mediator between groups such as participating countries to share information. Thus, the WHO arises as a center of translation. The actor-network theory emphasizes the structure susceptible to change (Callon, Law, and Rip 1986). Therefore, the ANT helps to find the limits of the network.

Moreover, network analysis provides theories and tools that generate puzzles about structures focusing on actor attributes (Arvanitis 2009; Hafner-Burton, Kahler, and Montgomery 2009). Networks serve as sets of actors sharing common interests on a specific issue and links through relations that form structures and enable agents (Hafner-Burton, Kahler, and Montgomery 2009; Krahmann 2005). The network approach defines a structure through patterns of relations between agents (Hafner-Burton, Kahler, and Montgomery 2009; Krahmann 2005). A network analysis links the nodes or agents, such as institutions and states, and connects to the liberal approach, which rejects nation-states as the only significant actor. Due to increasing interdependence, the process depends on institutional arrangements where nonstate actors are essential entities.

Collaborative networks foster communication and rely on openness to facilitate sharing (Clark 2020). Policy networks, in particular, are structured entities composed of relationships among diverse actors engaged in collective actions of mutual interest (Sandström and Carlsson 2008). However, understanding whether a network can have definable boundaries is critical for analyzing its operation and effectiveness. ANT helps to decipher the complexities of networks by examining mediations, which include places, regulations, and code programs (Latour 1999; Barnes 1979). Regulation, for instance, can refer to actions aimed at defining and transforming an organization's activities (Akrich and Méadel 2012) or as a "continuous collective learning process whose mechanisms remain partly implicit" (Akrich and Méadel 2012, 235). By considering actors within the network–such as WHO member states–and those external to it, such as China, cyber threat actors, and COVID-19, ANT enables a nuanced understanding of how networks are constructed and evolve.

Moreover, network analysis complements ANT by empirically assessing risks, vulnerabilities, resources, and relationships among actors. It provides a practical framework for understanding decision-making processes and identifying network boundaries. This approach is applied in the study to examine how actors in the GLASS framework collaborate to address global health challenges. While the methodological application of network analysis is further elaborated in chapter 2 (Research Design) and chapter 3 (Case Study), this section provides a foundational understanding of its relevance in exploring the dynamic interactions that underpin governance systems and security measures in global health.

Representative Reality of Surveillance Data

Individuals use different theoretical perspectives to predict or explain the future (Viotti and Kauppi 2020). The theoretical framework gives meaning to using *ingentis* data in a network surveillance system for infectious diseases within the health care industry. This investigation uses three concepts to ground the theories: complex interdependence, regimes, and security governance. The conceptual framework links the investigative process elements with the researcher's thought patterns, literature, interests, and methods (Ravitch and Riggan 2012). These international studies of concepts represent reality elements, open the black box (Latour 1987), and explain the challenges of public health in foreign policy. The concepts form the thematic focus of the research reported in this book and serve as chapter outlines-concepts that are the heart and the brain of this study and are described in detail in the following sections.

Regimes: A Complex Interdependent Dichotomy between Countries, Institutions, and Regulations

Understanding the foundational role of regimes prepares readers to explore how complex interdependence–a concept discussed in the following section–operates within these structures to address global challenges. A health regime's promotion originates from the need to report threats, such as pathogens, to maintain health surveillance and response capabilities. Scholars provide diverse definitions for regimes, often describing them as a set of principles, norms, rules, and procedures that guide collective action (Abbott and Snidal 1998; Haas 1980; Jervis 1982; Keohane 1984; Keohane and Nye 2012; Krasner 1982). These definitions underscore the role of institutions in coordinating activities regulated within the domain of international studies. For example, Ruggie (1975) characterizes regimes as broadly agreed-upon rules shaped by organizational commitments, while Haas (1980) frames them as procedural frameworks for issue regulation. Others highlight their legal foundation (Keohane 1982) or describe them as "rules of the game" (Bevir 2007) and patterns of behavioral norms that govern actors' interactions (Blanton and Kegley 2017; Krasner 1982; Puchala and Hopkins 1982; Jervis 1982). Through this lens, regimes serve as arenas where states interact efficiently (Abbott and Snidal 1998) and establish governance arrangements (Keohane and Nye 2012).

The interplay between regimes and complex interdependence is a central theme in international studies. Scholars explore this relationship between institutions and interdependence (Young 1982; Keohane and Nye 2012) by examining how institutions facilitate mutual expectations among actors within a regulatory framework (Ruggie 1975; Krasner 1982). Changes in these expectations often reshape the regimes themselves, as norms and principles evolve (Krasner 1982). The emergence of various types of regimes-from classical forms like aristocracy and democracy (Plato 1941) to modern iterations addressing security, health, finance, and technology-demonstrates their adaptability to address global challenges.

Regimes operate as knowledge-production systems, driven by diverse contributors such as micro-level human agencies, meso-level organizations, and macro-level institutional frameworks (Pestre 2012). These contributors foster transnational networks that address global issues, including sustainable development initiatives like the *United Nations Agenda 21* (Fontaine 2015). By addressing nontraditional security challenges, such as health crises, these networks highlight the critical role regimes play in fostering international collaboration.

Likewise, regimes underscore the interconnected and precarious nature of our world, described aptly as a "complex, interdependent, and dangerous world" (Puchala and Hopkins 1982, 245; Krasner 1982). Monetary investment and robust institutional frameworks mitigate the uncertainties associated with complex interdependence. For example, health surveillance regimes leverage global data-sharing mechanisms to combat infectious diseases, including AMR. Instruments of law like the International Health Regulations establish legal protocols for participating countries, guiding collaborative efforts to address global health threats. As Brousseau, Marzouki, and Méadel (2012, 16) state, "the position of some actors as gatekeepers makes them able to act as control points in the internet space or as governments' instruments of law." These regimes facilitate trust and reciprocity among states, encouraging cooperation to achieve shared goals despite inherent risks (Stein 2008; Krasner 1982). By positioning themselves as pivotal points within the global network, these actors contribute to the operationalization of regimes, ensuring a balance between security and collaboration in addressing global health challenges.

Furthermore, the presence of potential threats catalyzes the establishment of health regimes driven by shared global well-being and the need for heightened security measures. Security regimes are intricate and essential because of concerns about violations of common interests by other actors (Jervis 1982). However, the collective goal of addressing nontraditional threats holds greater value, as the cost of individualistic actions or national sovereignty can be perilous (Krahmann 2005; Jervis 1982). For instance, a security regime emerges when actors aspire to a regulated environment free from the fear of reprisal. These actors believe that mutual security is prioritized by all involved parties, creating reassurance and stability within the regime (Jervis 1982). Surveillance systems, such as those monitoring AMR, inform the formulation of policies aimed at addressing health security challenges (IACG 2019; World Health Organization 2019a). Open data-sharing practices foster trust among network participants, enabling collaborative action to combat infectious diseases. Thus, interdependence influences the establishment of stricter regimes, while complex interdependence promotes flexibility and adaptability among actors within the global regime framework.

Nevertheless, how have scholars differed in their discussions of the existence of an international regime? First, not all international regimes are designed to facilitate global communications (Krasner 1991). Some authors argue that regimes primarily function as state-centric mechanisms for understanding global politics (Strange 1983). Additionally, states often hesitate to collaborate within regimes, fearing that competitors may violate shared interests, potentially destabilizing security regimes (Jervis 1982). These fears stem from the risk of disrupting the balance of power or compromising state sovereignty. Scholars like Waltz (1979) and Jervis (1982) contend that regimes are constrained by the capabilities of individual states and the enduring anarchic structure of international relations.

While these countering perspectives question the efficacy and scope of regimes, incorporating such diverse viewpoints enriches the analytical depth of this study. By critically evaluating the limitations and challenges associated with regimes, this research highlights the importance of adopting a balanced and comprehensive perspective on their role in international relations. Incorporating the idea of regimes in this research highlights their role in fostering collaboration and managing interdependence, especially in addressing complex global challenges such as infectious disease surveillance. Despite their inherent limitations, regimes remain a crucial component of international relations, serving as platforms for structured cooperation and enabling governance frameworks to tackle shared security and health concerns. By addressing these debates, the study illustrates the necessity of regimes in navigating the intricate balance between state sovereignty and collective global interests.

To further understand the concept of an international regime, it is essential to recognize its foundation in international relations theory. An international regime refers to the principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue area (Krasner 1982). These regimes emerge from the need to address shared challenges, particularly in areas where unilateral action is insufficient. For example, the international health regime stems from the collaboration of states and institutions to combat infectious diseases that transcend borders. Scholars such as Keohane and Nye (2012) emphasize that regimes often arise in response to mutual interdependence, creating frameworks for cooperation that align with the interests of participating actors. Within the broader study of international relations, regimes provide a structured lens to analyze how actors interact within complex systems, balancing the tension between state sovereignty and collective security. By linking these broader theoretical insights to specific regional security complexes, such as the health regime facilitated by the WHO and the IHR, the analysis contextualizes the mechanisms that underpin global health governance.

Moreover, science requires cooperation to create shared understandings and solutions (Star and Griesemer 1989). Nation-states must perform together–or *cooperate*–to achieve common goals, which often result in the creation of boundary objects (Bowker and Star 1999; Star and Griesemer 1989). However, not all countries cooperate readily due to political, socioeconomic, or historical conflicts. Cooperation involves changes in each participant's behavior contingent on changes by others (Keohane 1988). Such changes illustrate the instability inherent in cooperative relations. Powerful nuclei at the core of these collaborations can sometimes harm society. Communicable diseases transcend national borders, and, more often than not, nation-states *co-labor* on shared objectives. Growing awareness of epidemics makes information-sharing more common because, as Bowker and Star (1999, 17) note, "microbes move rapidly across national borders and between large bureaucracies at an unprecedented rate." This shared effort highlights the power of boundary objects in bridging political, socioeconomic, and historical divides, fostering collaboration and advancing the global fight against infectious diseases.

A metaphor can help clarify the dynamics between collaboration and cooperation. Consider a symphony orchestra consisting of musicians, a conductor, and their instruments. The orchestra adheres to an agreed-upon script to create a musical masterpiece. Collaboration exists in the crescendo moment, where the sound reaches its peak, reflecting a collective effort. Cooperation, on the other hand, represents the individualized rhythm circle, where the musicians leave the process, but the music remains. In this scenario, collaboration provides a resolution, bringing the musical notes to their highest pitch and meeting the shared interests of the orchestra.

There is a growing tendency to involve multiple actors and adopt decentralized processes that engage diverse stakeholders, including experts, professionals, and citizens, to develop norms (Brousseau, Marzouki, and Méadel 2012). Regimes establish regulations such as the IHR, which encourage collaboration among participating countries and other actors (World Health Organization 2016a). Whether states choose to collaborate or not, the decision elevates security issues on the agenda. Transnational government actors such as the World Health Organization (WHO) and the World Trade Organization (WTO) play critical roles in regimes. States, as co-participants, have a voice in shaping agendas, while institutions provide platforms to organize summits and conferences (Fontaine 2015). This mutual contribution reflects a *quid pro quo* dynamic, benefiting all sides. For example, the WHO developed GLASS to facilitate the sharing of AMR reports among participating countries. The health regime also fosters collaboration through events such as the 'Artificial Intelligence for Good Global Summit' and the 'International Conference on Prevention and Infection Control.' These initiatives encourage participating countries to work together, advancing the shared goal of eradicating infectious diseases.

Complex Interdependence in Pandemic Threats

Over the past five decades, the politics of controlling infectious diseases, cybersecurity, and technology have evolved significantly. How do health politics align with the principles of complex interdependence within international studies? Complex interdependence, as outlined by Keohane and Nye (2012), is characterized by three core attributes: multiple channels of contact between societies, agendas comprising diverse issues not organized hierarchically, and a diminished role for the military (Keohane and Nye 2012; Pierre and Peters 2005). This framework suggests an international system where interactions among societies and states intensify, even as the prominence of military power diminishes. By contrast, interdependence reflects the interconnected relationships among actors and the system of their interactions (Coate, Griffin, and Elliott-Gower 2017). It highlights reciprocal effects between actors across nations (Keohane and Nye 2012), often marked by asymmetry arising from significant events or advancements in powerful states that influence others (Holsti 1978). Behavioral contingency, rather than reliance on *autarkic policies*, exacerbates power imbalances and global indifference (Coate, Griffin, and Elliott-Gower 2017; Holsti 1978). In this context, any substantial change in one actor inevitably affects others. Consequently, complex interdependence magnifies these interrelations, emphasizing the need for collaborative governance mechanisms in addressing global challenges.

This study shows that channels such as transnational relationships exist when participating countries contribute information obtained from surveillance of infectious diseases. The WHO plays a vital role in telecommunications between actors. The collaborative actor network includes international organizations, participating countries, governmental elites, representatives of the National Focal Points (NFP) surveillance centers, NGOs such as philanthropic organizations, private interest groups, foundations and companies, and the WHO's GLASS.

During the GLASS process, research shows a reduction of hierarchical power because military security does not dominate the GLASS agenda on the surveillance of infectious diseases. Is the GLASS database key to the collaborative link between different actors? The technology database does not transpire as a stand-alone thing. Digital technologies influence governance by facilitating the "management of the innovative processes of elaborating norms and standard," such as archives management (Brousseau, Marzouki, and Méadel 2012, 4). An organism has different meanings to those who use or identify it as a boundary object where many actors collaborate and interpret things differently (Star and Ruhleder 1996). Likewise, digital technologies also provide easier means to implement norms. For instance, "the control of access and code makes it possible to monitor how information and virtual spaces are accessed and used" (Brousseau, Marzouki, and Méadel 2012, 4). Thus, complex relationships define the use of technology.

Nonetheless, if the participating countries adhere to the IHR, each state freely tracks and reports its surveillance of threats in the form of pathogens. Similarly, governments participating in the GLASS and adhering to the IHR strengthen their national surveillance of AMR. In addition, participating countries generate quality data and share it globally, with an implied understanding that military force will not be used against other nations that are part of the network. These minor actions illustrate compliance with the IHR. Thus, a particular regulation enhances interests and combines resources for a specific *dispositif*.

The interweaving web of complex interdependence defines the GLASS as a channel connecting societies. How can heterogeneity or diversity in character and collaboration coexist when there are many global power players in data sharing, security, and management? Even though the GLASS database and IHR exist, they must manage infectious diseases adequately. What happens when a participating country needs more resources (time, space, or manner) to track and monitor the data? The costly reciprocal effects decrease when the interconnectedness between actors does not have significant expensive effects (Coate, Griffin, and Elliott-Gower 2017; Keohane and Nye 2012). This research shows limited interaction between participating countries during information exchange on bacterial pathogens that affect humans and on agents of AMR. The countries submit data to their respective NFP centers that input the relevant information to the GLASS network. Nevertheless, "microbes, objects, and techniques are a part of interactions" (Pestre 2012, 431). Therefore, infectious diseases become a boundary object because of the common interest in monitoring the threats among the actors.

Actor collaboration and interconnectedness with common interests do not involve high costs or increase interdependence. However, how does necessity illustrate a progressive movement toward promoting a health regime in a complex interdependent world? Complex interdependence exists because multiple channels interact for a higher cause. Likewise, it occurs when states mutually depend on other states for their well-being (Keohane 2012). A heightened security level is necessary because open data sharing can fall into wrong hands.

Nonetheless, direct cost accountability is part of the responsibilities of participating countries, which need to invest in surveillance tools and mechanisms to obtain the data. Any incurred costs vary between major and minor players and are a luxury that less developed countries cannot afford (Holsti 1978). Does the necessity of combating an infectious disease outweigh the cost of investment in surveillance tools? A complex interdependent world creates asymmetry. Collective action to prevent a global threat of pathogens outweighs the potential cost. However, participating countries may not have the means to implement and produce information faster than nonparticipating countries can. Likewise, even between participating countries, the lack of funds or accessibility to invest in high-technology surveillance systems may skew the reports. Herein lies the catch-22 of a complex interdependent world.

Other authors agree that complex interdependence includes "multiple transnational channels that connect societies" between elite governments (Viotti and Kauppi 2020, 399). States become dependent on transnational organizations that provide information (Nye and Keohane 1971). The state's agenda under complex interdependence consists of multiple problems not arranged precisely or in a stable and clear hierarchy (Viotti and Kauppi 2020). Furthermore, new resources of power affect the agenda (Keohane and Nye 2012). Marked by both continuity and change (Keohane and Nye 2012), the world continually evolves. Every new threat opens the door for collaborative efforts to combat global issues. Groups that disrupt the network have their plan and strive for hegemonic dominance in technology or industrial capital.

The interconnection of actors contributes to the development and refinement of AI applications. Specifically, data scientists and engineers collaborate within networks to enhance AI models, leveraging *ingentis* data for building robust mechanisms and improving their applications across various fields. The technological revolution in AI, fueled by the exponential growth of big data, continues to reshape the international landscape. However, with advancements come potential risks. Nonconventional threats, such as the misuse of AI, biological weapons, cybersecurity breaches, and emerging technologies, alter the priorities of global security agendas. While complex interdependence often deprioritizes national security (Coate, Griffin, and Elliott-Gower 2017), politicization frequently elevates it as a critical issue (Keohane and Nye 2012; Guzzini 2011; Ruggie 1975). For instance, infectious diseases transcend borders, compelling states to view global health as a matter of national security. Similarly, the growing prevalence of cyberattacks positions these threats at the forefront of political agendas. In this context, national security becomes not only a vital consideration but also a due diligence checkpoint within the broader political network equation, emphasizing the need for adaptive strategies and collaborative solutions.

Institutions provide enhanced telecommunications and information flow, reduce uncertainty, and provide avenues for agenda-setting and bargains (Coate, Griffin, and Elliott-Gower 2017; Holsti 1978). For example, the WHO raises global health issues on the agenda that otherwise would not be relevant. However, does the WHO have sufficient power to influence global actors when external demands, heightened security threats, and technological advances are high? The WHO relies on "member states' funds, votes, and recognition" (Chorev 2012, 226). If an institution depends on funding and outside sources, does such dependence lessen its character as a power influencer in a complex and interdependent world? Nonetheless, with global threats beyond the ambit of normal human existence, such as a pandemic, the dynamics of power play between states and institutions are blurred. Governments are unlikely to face traditional security as a principal issue (Keohane and Nye 2012). Security considerations cannot be swept under the rug with international data sharing, even with publicly available technology. Such open data leave the door open to potential outside threats.

Furthermore, the political agenda shifts the focus away from military security, and governments do not use military force against one another (Viotti and Kauppi 2020). However, new threats divert attention away from concerns related to the military (Keohane and Nye 2012). The information revolution influences the international system and alters the scope of complex interdependence. Keohane (1998) indicates three types of information as a power source: information commercially provided at a price, valuable contained strategic information unless placed in the wrong hands, and free information, which actors create without compensation. The information shifts the patterns of complex interdependence and increases communication lines amongst actors in the network (Keohane

1989). This study shows that communication increases when an institution develops a technology database and participating countries input information on the surveillance of infectious diseases.

Complex interdependence illustrates the intricate ties between actors in collaborative efforts to address nontraditional threats. Communication channels expand when countries voluntarily participate in collaborative networks. For example, an institution's or state's agenda might focus on global health challenges such as monitoring bacterial pathogens that affect humans and surveilling AMR, which the World Health Organization (2020b, 2017b) has identified as one of the top ten critical global health threats. Under such circumstances, the military does not dominate the agenda, allowing complex interdependence to provide a framework for exploring solutions beyond traditional hierarchical norms.

Although complex interdependence aligns more closely with contemporary global realities than realism (Keohane and Nye 2012), the latter remains significant for understanding state-driven power dynamics. Realism focuses on the anarchic nature of the international system and the centrality of state power; however, it often overlooks the increasing interconnectedness and interdependence of modern global challenges, such as health crises and cybersecurity. Haas (1975) argues that imbalances within complex interdependence can reduce interconnectedness, while Banks (1985) emphasizes the enduring relevance of state power and military force. Similarly, Waltz (1979) posits that the international system retains an anarchic structure that shapes interactions among major global powers. Holsti (1978) highlights how significant geopolitical shifts or disruptions in collaborative networks can challenge the continuity of complex interdependence. By integrating alternative views, this study strengthens its theoretical foundation, demonstrating how the chosen framework, complex interdependence, addresses the gaps left by realism. Acknowledging counterarguments also enriches the analysis, highlighting the unique adaptability of complex interdependence in accounting for the collaborative networks and diverse actors essential for addressing nontraditional threats. This comprehensive approach underscores the importance of moving beyond a singular theoretical perspective to understand the complexities of a globalized, interconnected world.

The conditions for further developing complex interdependence remain promising. Established behavior patterns within international organizations often create resistance to change (Keohane and Nye 2012; Holsti 1978). However, evolving challenges demand adjustments in institutional collaborative networks to better address contemporary global threats. Complex interdependence, by promoting a health regime, collaborative actions, and interconnectedness within actor networks, provides a pathway to navigate these challenges. It bridges the gap between theory and practice, demonstrating its capacity to guide real-world responses to global health crises and foster a more complex, mutually reliant world.

Security Governance in the Control of Infectious Diseases and Data through Open-Source Intelligence Technology

As the world experiences increasing globalization and rapid advancements in transportation and communication, the concept of traditional security is being transformed. Technological progress prompts contemplation of the intricacies of a complex and interdependent society. The emergence of new threats transcends the traditional focus on state dyads (Kirchner and Sperling 2007), now encompassing a wide array of actors, including society, individuals, and states.

Scholars define governance as the “reflexive self-organization of independent actors involved in complex relations of reciprocal interdependence” (Jessop 2003, 101). This concept emphasizes ongoing dialog and resource-sharing to develop mutually beneficial ideas, while managing inherent contradictions (Brousseau, Marzouki, and Méadel 2012). In this context, security governance is conceptualized as a system of rules devised by actors to collectively manage their existence in response to threats (Breakspear 2013; Bevir 2007; Krahmann 2005; Webber et al. 2004).

Security threats arise when there is a potential negative impact on the welfare of individuals, society, or the state. The characterization of a security threat is based on criteria such as probability, specificity, scope, and seriousness (Kirchner and Sperling 2007; Krahmann 2005). Thus, global recognition of security governance contributes to the promotion of a health regime.

Most people object not so much to opening the black box of a health regime and analyzing its contents as to the surveillance itself (O'Neil 2016). Infectious diseases affect human survival. An economy cannot be mobilized without its citizens or a community. Moreover, new security threats emerge, such as contagious diseases, which change the landscape of security and push the emergence of security governance given the evolving nature of threats (Krahmann 2005; Bowker and Star 1999). Likewise, different governance types exist in the international system, such as democratic, centralized, traditional, and administrative, and those acting in the state's name (Fontaine 2015; Kooiman 2002). Therefore, governance depends on the interaction and process of multiple players, such as state and nonstate actors, public workers, and socioeconomic actors.

Scholars use such common words to define governance as system, set, form, mechanism, or regulation process in determining state affairs. Some note that governance acts as a system of rules accepted by the majority (Rosenau 1992) and regulates the situation arising through immediate information and arrangements between actors for policy action (Fontaine 2015; Webber et al. 2004). Other authors contend that governance serves as a system of regulations to motivate public and private institutions and to manage their everyday affairs (Bevir 2007; Webber et al. 2004). Others describe governance as a set of processes and institutions guiding international surveillance (Keohane and Nye 2012; Viotti and Kauppi 2020). Some other authors note that governance indicates a fragmented network that structures collaboration, mode of policymaking, and collective group activities to help society adapt to change and attain those goals (Breakspear 2013; Krahmann 2005; Pierre and Peters 2005). The governance structure enables an organization to anticipate change, open windows of opportunities, or avoid the harmful effects of threats (Fontaine 2015; Breakspear 2013).

Furthermore, recognizing a legitimate problem implies that actors place a particular hierarchy level on multiple existing issues and select the most urgent ones (Fontaine 2015; Pierre and Peters 2005). Moreover, other scholars define security governance as "a system of rule conceived by . . . actors aiming at coordinating, managing, and regulating their collective existence in response to threats to their physical and ontological security" (Adler and Greve 2009, 64; Liao 2012; Kirchner and Sperling 2007). At the same time, other authors indicate that national elites strive for flexibility in the governance of international security by eschewing war as a state-crafted instrument. Meanwhile, yet others accept that the benefit of security governance outweighs a declaration of war and respect the existing situation (Kirchner and Sperling 2007; Keohane 2002). Thus, international organizations such as the UN and the WHO encourage or promote decision-making and influence the subject's importance.

The literature further suggests that security governance works to secure a health regime because governance identifies vulnerabilities to understand the structure of interdependent relationships and the actors that set the rules of the game, *ceteris paribus* (Latin for 'all other things being equal') (Keohane and Nye 2012). In an increasingly complex world in matters of the organizations of governance, "technical capabilities are the source of new legitimacies and new capabilities, and, hence, new potentialities and needs" (Brousseau, Marzouki, and Méadel 2012, 7). Complex interdependence faithfully reflects how security governance promotes regimes on the surveillance of infectious diseases by understanding global relations between actors in a collaborative network. The present research analyzed economic pressures, greater new security threats, and wider transnational contacts (Krahmann 2005, 2003). Furthermore, the focus of the study includes the development of security governance and its five features: heterarchy, the interaction of a large number of public and private actors (depending on the issue), formal and informal institutionalization, ideational relations, and collective purpose (Webber et al. 2004). Specifically, the concept of security governance involves

> [c]oordinated management and regulation of issues by multiple and separate authorities, the interventions of both private and public actors (depending upon the issue), formal and informal arrangements, in turn, structured by discourse and norms, and purposefully directed toward policy outcomes (Webber et al. 2004, 4).

Heterarchy characterizes governance and suggests various coordinated actions and the absence of central political power. It entails the presence of multiple positions of authority in a security space (Sperling and Webber 2014) and is composed of more than just self-regulated actors and spaces (Brousseau, Marzouki, and Méadel 2012). The heterarchy complexity defines new interaction patterns through collaboration and interaction between actors. In the context of the second dimension, interactions, the focus of attention is on the involvement of many connected actors in a regional and sometimes global setting. The third dimension, namely, formal and informal institutionalization, indicates the institutionalization of rules and norms that identify legitimate actors and set the boundaries of behaviors through committees, meetings, or institutional initiatives. The fourth dimension involves ideational relations between actors that engage in common acts structured around addressing a particular issue (Sperling and Webber 2014; Webber et al. 2004). Lastly, the fifth dimension, collective purpose, maintains that security governance is about achieving a collective goal and the collective process by which actors achieve the goals (Sperling and Webber 2014; Rosenau 2000). Thus, while conducting the present case study, these five valuable features assisted in analyzing the collaboration in sharing data on the surveillance of infectious diseases.

This study shows that global health security recognizes infectious diseases as a threat. The theoretical perspectives serve as tools to analyze new forms of security threats appropriately and provide alternative ways to address the issues by collaborating with diverse actors (Liao 2012). Furthermore, the collaboration of states through the IHR, an international legal instrument, contributes to the security governance of massive amounts of data obtained through publicly available information obtained from the surveillance of infectious diseases. At the same time, security governance keeps the traditional state-centered security structure. Thus, the conceptual analysis strengthens state functions when analyzing international relations among nonstate actors.

The subsequent chapters measure the perception of nontraditional security threats, such as infectious diseases, and secondary threats, such as cyberattacks and emerging technologies. For example, nonconventional threats develop during the security governance process on the surveillance of infectious diseases to promote the emergence of a health regime. Thus, an open-source intelligence database harmonizes data sharing to promote global health.

Insights from Multiple Fields and Disciplines

This section integrates perspectives from three interconnected fields: sociology of technology, international law, and the combined domains of cybersecurity and intelligence. Together, these fields provide complementary perspectives that inform the central research question: Through the OSINT technology database of the WHO, why did security governance promote the health regime on the surveillance of infectious diseases in the Americas from 2015 to 2021? By drawing insights from these areas, this study bridges theoretical understanding and practical applications, offering a multidimensional perspective of the challenges and opportunities inherent in global health governance.

Sociology of Technology: Codes, Algorithms, and Artificial Intelligence

What collaborative norms are essential to addressing the international security dimensions of technological innovation? How does technology act as a catalyst for social transformation? While the notion of a singular solution or universal norm (a technological *panacea*) may seem idealistic, practical solutions are more likely to emerge through dynamic, iterative processes.

The sociology of technology examines how nonhuman actors–such as the code of international law (a mechanism for social governance), algorithms (a structured set of operational rules), and artificial intelligence (AI, systems capable of performing tasks requiring human intelligence)–contribute to reshaping networks and societal norms. These actors do not operate in isolation but rather as integral components of collaborative networks. For instance, the code regulating access to virtual spaces enables the monitoring and management of information flows, ensuring that digital technologies foster transparency and accountability (Brousseau, Marzouki, and Méadel 2012). This interplay highlights how digital technologies shape the interactions between human and nonhuman actors, advancing the implementation of norms and enhancing accountability within interconnected networks.

An analysis of these elements illustrates how they support the creation of relationships among human and nonhuman actors. The interplay between actors within these networks enhances global health surveillance and fosters innovation. For example, codes standardize data sharing protocols, algorithms process *ingentis* data to identify trends, and AI accelerates decision-making processes. These interconnected elements collectively promote a deeper understanding of the complex interdependence between actors and how technological innovations contribute to addressing shared global challenges.

Including this interdisciplinary lens strengthens the analysis by contextualizing the role of technology as a transformative force within security governance. While these tools offer significant benefits, they also highlight vulnerabilities, such as unequal access, biases in AI, or misuse of data. Thus, this review provides a critical framework for understanding how human and nonhuman actors collaborate to build resilient systems capable of managing the complexities of infectious disease surveillance and response.

The code of law and technology evolve rapidly, reflecting the complexities and unpredictability of the modern world (Pierre and Peters 2005). In jurisprudence, legislation represents the code of law, while in cyberspace, operations rely on software built from programming codes (Balzacq and Cavelty 2016). Both legal and software programming codes function as nonhuman actors, shaping political relevance, perceptions, and abstract frameworks such as security governance, regimes, and complex interdependence. These codes are embedded with purpose, influencing how society interacts with and perceives governance and regulatory systems. While technology facilitates the production and dissemination of knowledge, political and legal institutions remain the primary forces shaping societal structures and norms (Jasanoff 2004). Additionally, technology generates knowledge through the interplay of interdependent technical objects, including material, information, and the contributions of human actors like engineers and scientists (Arvanitis 2009). This perspective treats both human and nonhuman *actants* equally, emphasizing their collaborative roles in shaping the socio-technical landscape (Pestre 2012). By acknowledging the influence of these codes and their role as actants, this study underscores the importance of understanding their impact on interconnected governance systems and global security.

Likewise, technical objects build diverse networks, which bring together human and nonhuman actants (Akrich 1997). Boundary objects appertain to the negotiation process because each actor knows what the object means to itself in a shared infrastructure (Bowker 2000). Open-source information and transparency lead to a collaborative movement between nations. On the one hand, codes, rules, and regulations drive the urgency to keep up with actors' interdependence. On the other hand, technological changes necessitate conformity to a growing society. A new generation of individuals governs a contemporary culture of progress and contributes to the knowledge infrastructure. In the social sciences, computer technology allows greater communication and interdependence, contributing to technological innovations. Advancements in technology increase interconnectedness, and "technological innovations increase the individual and collective well-being" (Beck 1992, 184). Both technical and legal codes affect the political and social realm, regulate space and behavior, and work within the norms of virtual space to analyze information on a large scale (Balzacq and Cavelty 2016; Lessig 2006). Thus, codes mediate the realm between law and technology.

Likewise, algorithms constitute part of the database that makes up the framework within the technology ecosystem (Webb 2019). Nevertheless, bias influences the shape of algorithms and the development of information infrastructure. Who are the creators behind the algorithms that serve as inputs into the database? How are they creating actors and redefining the world? This study questions the GLASS as an object because algorithmic bias skews the security and the level of intelligence analysis by reshaping what actors consider as a threat in the interests of national security.

In addition, emerging technologies pose threats or comprise powerful enabling capabilities that operational end-users deploy (U.S. Department of Homeland Security 2020). Whereas the focus lies on global health and cyber issues, other emerging technologies, such as AI, have entered the field. By 2026, the AI market is expected to increase to approximately $53.1 billion and a compound annual growth rate (CAGR) of 35.4% between 2019 and 2026 (Anzivino, Anfossi, and Saracino 2021). Thus, monitoring emerging technologies enhances analysis, increases the accuracy of prediction, and reactivates the capacity to acknowledge foreseeable threats.

Mechanisms of AI, such as machine learning, automate a vast amount of information that quickly and efficiently assesses data. In its most rudimentary explanation, AI is the engineering of developing intelligent machines to understand human intelligence through biologically observable methods (McCarthy 2007). Artificial intelligence also refers to a "set of computer science disciplines aimed at the scientific understanding of the mechanisms underlying thought and intelligent behavior and the embodiment of these principles in machines" (U.S. Congress. Senate 2016, 9), which deliver value to people and society. Similarly, the National Security Commission Artificial Intelligence Act of 2018 defines AI as "an artificial system designed to act rationally, including an intelligence software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting" (Congress.gov 2018, 8). The diverse, interconnected group of actors in the network, coupled with new technologies from AI mechanisms to algorithms in the GLASS platform, influence change in combating the threat more than any other cohort.

As a subset of AI, machine learning depends on the researcher or scientist to judge and guide the process and assess intermediate results (Kitchin 2014). Machine learning helps recognize patterns, predict threats, identify big data and spam, and classify malware (Gibert, Mateu, and Planes 2020). Computer algorithms make use of significant amounts of data through machine learning or automated processes, spot patterns, and generate theories (Steadman 2013). Algorithms work on big data to discover associations between data without the guidance of a hypothesis (Kitchin 2014, 22). Therefore, big data are necessary to establish a surveillance system for infectious diseases.

Algorithmic bias exists when a data scientist introduces issues that train the machine learning system. By contrast, a person creates algorithms with unintended cognitive biases since "neither may a programmer whose program behaves differently from what he had intended look for the fault anywhere but in the game he has himself created" (Weizenbaum 1976, 112), nor may they seek the fault in external factors. Likewise, "considerable flaws and biases can exist in the algorithms that support AI systems, calling into question the accuracy of such systems and its potential for unequal treatment" (U.S. Congress. House of Representatives 2018a, 3). A potential method to identify algorithmic bias obtained from an intelligent machine includes hiring auditors to offer algorithmic scrutiny, which helps to mitigate how analysts conduct intelligence (Danks and London 2017; O'Neil 2016). Therefore, perceptions provide an avenue of added information to comprehend reality.

Nevertheless, what is the ideal modus operandi for governance to keep up with emerging technology? Emerging technologies pose security concerns when they shorten distances and create novel and extraordinarily effective means of destruction, which threaten humankind's security and survival when placed in the hands of nations that claim unrestricted freedom of action (Einstein 2011). However, excessive regulation stifles the growth of global health and digital services by over-regulating.

Although advancements in technology have not made us inherently superior to our ancestors, due to the presence of bias resulting from the natural tendency of the brain to seek connections it is crucial to acknowledge the potential ramifications of genetic engineering, a technology-driven field, which "could result in major social disruptions worldwide during coming decades" (Clark 2020, 280). Consequently, despite the benefits brought in by the accelerated pace of technology, technology-driven systems introduce uncertainty in strategic planning and unintended consequences.

Emerging technologies, such as AI, use their implements exponentially, which brings about new opportunities and challenges. Artificial intelligence "drives information enhancement, helps interpret information, provides answers at the speed of light" (Sanclemente 2021, 7). Raising awareness of the potential pitfalls of emerging technologies and other topic-relevant actors creates a better security process for the intelligence community[2] analysis in the interests of national security. Thus, the key to addressing questions, opportunities, and challenges includes a collection of diverse actors and approaches from the bottom-up to the top-down with mindfulness to obtain solutions cautiously.

Artificial intelligence influences a network and the speed with which information is shared between actors. Digital technologies and AI protect society from health emergencies and open the door to nonconventional threats, such as cyberattacks and hacking. Artificial intelligence plays an essential role in the surveillance of infectious diseases and defenses against outbreaks. In particular, AI mechanisms progress exponentially, reaching not only the most developed countries but also the most remote villages (Glauser 2018). Skeptics of change and fear of AI mechanisms drive significant transformational change, which intersects various life areas from health to security to finance. For example, the GLASS technology database lacks AI mechanisms to capture AMR data (World Health Organization 2017b). However, harnessing emerging AI technologies leads to effective sharing of AMR data, diagnostic mechanisms, and analytical and assessment tools (Ashley et al. 2019). Automatic data harmonization between laboratories, participating countries, and institutions provides effective scale-up, integration, and translation (Ashley et al. 2019; Callon, Law, and Rip 1986).

Moreover, AI significantly improves response to disease outbreaks by issuing early warnings, forecasting epidemics, and enhancing decision-making for simulation tools and responses to outbreaks (Ghebreyesus 2018). Therefore, the WHO supports AI and implements safeguards. While the GLASS platform does not incorporate AI mechanisms per se, the WHO's stance on AI indicates its future potential for the surveillance of AMR. Nonetheless, codes, algorithms, high-performance computing, and AI mechanisms contribute to the notion of frontier objects, co-production, and interdependent

[2] The term *intelligence community* used in this study refers to the U.S. Intelligence Community, composed of 18 different organizations. See Office of the Director of National Intelligence at https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

activities in the actor network (Star 2010; Arvanitis 2009; Jasanoff 2004; Latour 1993; Callon, Law, and Rip 1986). The mechanism stems from the response, transmission, and contribution to knowledge production.

Moreover, co-production allows the sorting of hybrid networks between state and nonstate actors (Jasanoff 2004; Latour 1993) and clarifies different levels of the social order, such as health regimes, to drive global health and security. Natural technical objects (GLASS and IHR) and social objects (the WHO and participating countries) interweave in the actor network on the surveillance of infectious diseases. How do these material objects and institutions assign hybrids to their constitutional domains? The objects grant agency to nonhuman and human actors, which provides content regarding theoretical knowledge and technical objects (Jasanoff 2004; Latour 1993; Callon, Law, and Rip 1986).

Cybersecurity plays a pivotal role in shaping and regulating objects in cyberspace by identifying vulnerabilities, developing protective measures, and fostering collaboration among stakeholders. The increasing complexity and proliferation of digital processes in cyberspace across the globe underscore the vast scale and severity of the challenges associated with ensuring cybersecurity and managing technological advancements. Initially, the internet posed significant challenges to regulation due to its decentralized nature and lack of standardized frameworks. Over time, however, "after years of standardizing protocols and digital languages, cyberspace has become an increasingly sophisticated site of regulation" (Albornoz 2020, 46). A global commitment to multilateral, public, and private cooperation on technological advancements could significantly improve digital access and security. The internet, predominantly owned and operated by the private sector, exemplifies this dynamic, as citizens and governments alike rely on technologies developed by private entities. These realities underscore the critical role of public-private collaboration in addressing cybersecurity challenges and ensuring the secure and equitable use of digital technologies.

In response to cyber threats, actors track millions of data points across their infrastructure. As a result, threats to critical items of infrastructure are rendered ineffective by isolating those items, whereas threats to cyberspace occur in a common medium such as a network or the internet. Moreover, cyberspace opens a range of power projection tendencies to manipulation, whether in the social, public opinion, or technical sphere, when threats target critical infrastructure, governance, and legal frameworks tailored to serve the interests of a coercive community, creating challenges. Therefore, much of the manipulative activity poses the risk of falling through the cracks and thereby remaining undetected.

The sociology of technology provides a reinforcing framework for theories and concepts. It raises risk factors in technologies and security issues against nonconventional threats, such as attacks using biological weapons, cybersecurity, and emerging technologies. Furthermore, technological advancements spread interdependence between the social and material complex world because data grow exponentially. Thus, the sociology of technology provides a reinforcement mechanism for promoting a health regime.

International Law: Uniting Actors with International Health Regulations (2005)

International law assists in dealing with conflicts between nation-states. It provides order during times of chaos and plays a vital role in the structure of the international system given the law's ability to respond to global change. The society of nations includes recognizing rights and does not obliterate the human demand for justice (Grotius 1901). The International Health Regulations (2005) provide the legal framework for handling public health emergencies of global concern and link the state to the legally binding instrument that provides guidelines on responding to those concerns or emergencies.

On May 23, 2005, the World Health Assembly (WHA) adopted the IHR, a legally binding instrument that came into effect on June 15, 2007 (World Health Organization 2016a). The regulations emerged in the context of an ever-increasing interconnected and interdependent world. Countries need to respond in a timely fashion to prevent threats to public health (Kluge et al. 2017), and the IHR seek to prevent, protect against, control, and provide appropriate response to check the spread of diseases across countries or nation-states (World Health Organization 2016a). Thus, the IHR encourage collaborative approaches toward global health and engage different actors.

Public policy refers to the laws, governmental actions, funding priorities, and regulations that reflect given positions, attitudes, cultural ideals, or accepted rules (Kilpatrick 2004). The policy processes information delivery to help in carrying out practical tasks (Dryzek 2008) and sets specific measures (Page 2008). For example, spreading infectious diseases paves the way for nontraditional threats, such as using pathogens in a biological warfare. *Bacillus anthracis* (otherwise known as the anthrax pathogen), Ebola, *Aspergillus fungi*, and other similar infectious diseases or pathogens have destructive tendencies. The regime to prohibit biological weapons in the multilateral disarmament treaty at the 1972 Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological and Toxin Weapons and their Destruction implements prohibitory norms against biological warfare (Kelle 2007). The convention supplements the Geneva Protocol, which came into force in 1928, which prohibits chemical and biological weapons (Kelle 2007; World Health Organization 2004). Regulatory tools encompass post-marketing surveillance systems, organized by administrative or professional bodies such as the U.S. Food and Drug Administration (FDA), which rely on court decisions that influence users' choices, doctors' prescriptions, and regulatory authorities (Gaudillière 2014). Moreover, regulatory policies serve as an instrument that contributes to decision-making processes, since public policy decisions are co-produced by a plurality of actors with different values and objectives (Fontaine 2015). States, guided by their enlightened self-interest (Viotti and Kauppi 2020; Grotius 1901), adhere to established norms influenced by the law's instrumental role. Therefore, regulatory policies help maintain order, prevent chaos, and prohibit behavior that endangers a nation and its citizens.

The spread of more legal institutions and practices tackles various issues, from infectious diseases to cybersecurity and emerging technologies, and raises concerns about jurisdictional privacy laws and legal globalism (Keohane and Nye 2012). A potential reference to complex interdependence encompasses change from technology to legal industries. When an extensive database integrates information from diverse international sources, the potential for data abuse increases exponentially (Bowker 2001). Institutions serve to reaffirm political culture. The legal system allows institutions more weight, a repertoire of solutions to problems, and methods to secure their credibility and manage dissent (Jasanoff 2004). Leadership and governance are paramount in improving the implementation of the IHR and the cornerstone of any effort to strengthen health security (World Health Organization 2016a).

Moreover, the IHR illustrate regimes because, as a binding international legal agreement, the IHR help countries work together to enhance public health security. Nonetheless, a regime lacking formal legality cannot command our allegiance (Kant 2006). An international society considers international law an institution since international law includes international regimes (Keohane 1988; Bull 1977). The International Health Regulations relate to the emergence of a health regime because IHR establish rules to support global outbreaks such as infectious diseases and strengthen national surveillance. Rules remain important regulators to govern information in cyberspace to ensure intellectual property rights, and legal text mobilizes other instruments (Fontaine 2015; Keohane and Nye 1998). Therefore, the IHR serve as an essential legal instrument. They ensure health security on the security governance of data sharing and infectious diseases. Through open-source intelligence on the surveillance of infectious diseases, the possibility of promoting a health regime exists because diseases go beyond national borders.

Cybersecurity and Intelligence: Managing Risks in Global Health

Traditionally, national security interests include threats other than those of infectious diseases. For instance, in the United States, environmental degradation and bioterrorism were not perceived as national security interests (Hodge and Weidenaar 2017) and cross-border transmission of infectious diseases did not typically involve military balance of power

(Fidler 2003). However, owing to the rapidly changing times, the exponential growth of data, and the emergence of new threats, the landscape and scope of national security interests have expanded to encompass novel challenges. Does the health paradigm become a determinant of war or a conflict starter? Such a paradigm is an object of further articulation (Kuhn 1996). Within Kuhn's paradigmatic framework, the application of factual knowledge in the pursuit of groundbreaking investigations has significantly contributed to the advancement of research on infectious diseases and bolstered strategies related to national security (Kuhn 1996). Therefore, actors push the boundary object of science to address pandemics and security crises to facilitate communication and collaboration between policy making and public discourse.

Intelligence reduces uncertainty and does not exclude the use of open-source information. The competence of analysis, such as open sources, reveals information that opponents wish to hide (Clark 2020; Kent 1965). The internet also provides leaders and communities with the "ability to organize themselves and to benefit from the distributed intelligence that lies in the network" (Brousseau, Marzouki, and Méadel 2012, 6). In the context of cybersecurity, intelligence plays a vital role in identifying vulnerabilities within digital infrastructures, detecting emerging threats, and developing strategies to mitigate cyber risks. Cyber intelligence analyzes patterns of cyberattacks, uncovers the tactics of malicious actors, and supports proactive measures to protect sensitive information. Likewise, intelligence establishes facts, provides valid inferences such as hypotheses or conclusions, and strives for impartial analysis (Clark 2020; Kent 1965). As cyberattacks increase in frequency and sophistication, the integration of intelligence into cybersecurity frameworks becomes indispensable in safeguarding critical systems and fostering trust in digital environments. Thus, intelligence connects to the complex process of understanding meaning in available information, whether applied to traditional security challenges or the dynamic, ever-evolving realm of cyberspace.

Likewise, within the field of intelligence studies, the focus on national security traditionally prioritized certain topics over others, such as infectious diseases, bioterrorism, and environmental degradation. However, the scope of national security interests has expanded to encompass new nonconventional threats due to technological advancements, changing times, and the emergence of novel risks. Additionally, scholars have highlighted the interconnectedness between infectious diseases, national security, and cybersecurity concerns. We inhabit a world where interconnectivity spans the entire spectrum, surpassing borders, which no longer astonishes us (Carril 2020). Infectious diseases disregard boundaries and easily traverse geographical borders.

Traditionally, intelligence follows a cyclical process that includes identifying requirements, planning, collecting information, processing data, conducting analysis, and disseminating findings (Clark 2020). However, in larger organizations, this cycle often becomes nonlinear, with officers revisiting collection and analysis phases based on evolving needs (Kent 1965). While this traditional cycle provides a framework, intelligence work often involves abstract, iterative processes that adapt to the complexity of modern challenges (Clark 2020). In the context of global health and cybersecurity, intelligence studies intersect with efforts to secure open-source data and analyze threats to health surveillance systems. For example, as platforms like GLASS facilitate data sharing across borders, they also highlight vulnerabilities that intelligence and cybersecurity measures must address to prevent exploitation by malicious actors. Cybersecurity plays a critical role in identifying, mitigating, and preventing threats such as data breaches, ransomware attacks, and misinformation campaigns that could compromise the integrity of health surveillance systems. Additionally, cybersecurity frameworks, including encryption protocols, access control mechanisms, and real-time threat monitoring, provide essential defenses against the misuse of sensitive health data. This convergence of intelligence and cybersecurity underscores the need for adaptive frameworks that secure data integrity while fostering international collaboration and ensuring the resilience of critical health networks.

Intelligence exists in both the traditional and nontraditional sense. For example, the type of techniques used determines the difference between intelligence officers and professional scholars. Scientific laboratories collect information to reduce uncertainty. Laboratories in academia would not send information that includes intercepted telephone communications, concealment, or deception. Professional scholars train "in the techniques of guarding against their intellectual frailties" (Kent 1965, 199). Intelligence supports a range of operations such as military planning, diplomatic and trade negotiations, policy, law enforcement, and cybersecurity (Clark 2020). In intelligence, the type of customers acting on the information varies and may include decision-makers, executives, policymakers, law enforcement officials, and unit commanders of military operations (Clark 2020; Kent 1965). The propensity to use intelligence also varies by industry: business leaders and customers of competitive or strategic intelligence are more inclined to use intelligence. The interweaving of cybersecurity and intelligence practices has become essential, particularly for protecting critical data infrastructures and ensuring secure communication channels in the face of growing cyber threats.

Cybersecurity significantly intersects with intelligence, particularly in the safeguarding of sensitive data within global health networks like the GLASS framework. As cyber threats increasingly target health surveillance systems, cybersecurity plays a pivotal role in protecting the integrity and confidentiality of data shared across borders. This includes implementing robust encryption protocols, monitoring for unauthorized access, and detecting attempts to de-anonymize data or exploit vulnerabilities in health networks. For instance, the global AMR surveillance system, with its publicly accessible tracking framework, provides valuable insights to intelligence analysts and the broader intelligence community, reducing uncertainty in monitoring and responding to infectious diseases. Other actors that benefit from participating in GLASS or similar health surveillance networks through data sharing include nation-states (World Health Organization 2017b), multilateral agencies (Edelstein et al. 2018), and cybersecurity experts working to prevent cyberattacks on these systems. Thus, surveillance networks such as GLASS aid a diverse range of actors while underscoring the need for integrated cybersecurity measures to enhance resilience and trust in the shared data.

Literature shows a connection between U.S. national security and global infectious diseases (Hodge and Weidenaar 2017; Cecchine and Moore 2006). For instance, in the United States, the National Biosurveillance

Integration Center (NBIC) based in the U.S. Department of Homeland Security (DHS) Countering Weapons of Mass Destruction Office (CWMD) analyzes and shares information about biothreats, emerging diseases, and infectious disease surveillance (U.S. Department of Homeland Security 2022). Likewise, APUA-Brazil in Brasilia promotes the control of AMR at the global level. Moreover, cyber threats challenge institutions, security governance, and laws because of concerns of the growth of adversarial technical knowledge that enhances threats to the security of the economy and the health of nations (U.S. Director of National Intelligence 2019). Emerging technologies, such as AI and high-performance computing, pose a threat when placed in the hands of military and intelligence adversaries (U.S. Director of National Intelligence 2019). The information environment within an intelligence community includes different actors, from individuals to organizations, which have the capacity to collect, process, and share information following law and policy (U.S. Director of National Intelligence 2019).

Secondary threats, such as climate change, add to enhanced security measures and the scope of intelligence analysis. In 2015, health officials reported the spread of the Zika virus in Brazil. By 2016, more than a million Brazilians had been infected, and it was speculated that inclement weather and poor water and drainage infrastructure had facilitated the spread of the virus (Lakoff 2017). Environmental problems recognize no frontier. For instance, malaria, an infectious disease, is sensitive to long-term climate change, involving high humidity and rainfall for example (Arvanitis 2009). In addition, global attention increases because infectious diseases add to other security concerns (Cecchine and Moore 2006). Thus, a link exists between the transmission of infectious diseases, climate, and cybersecurity.

Societies value health and human security but misunderstand their connections and interdependence (Chen and Narasimhan 2003). Nonetheless, some authors concur on the links between national security and health, whenever national interests are substantially threatened by infectious diseases (Cecchine and Moore 2006; Brower and Chalk 2003). Compared to other threats to national security, the former U.S. White House Homeland Security Adviser declared that infectious diseases pose the greatest danger to national security (Lakoff 2008). Implications for national security arise when such threats increase significantly and cause devastating global harm to health, life, and human security. Infectious diseases remain an existential threat that affects one nation and multiple channels that spread beyond national borders. Transparency enhances public trust and facilitates decision-making on information available through open sources while protecting information that harms national security (U.S. Director of National Intelligence 2019; Hodge and Weidenaar 2017). Greater state transparency remains indispensable in the security governance of infectious diseases and perceptions of nonconventional threats.

Furthermore, when the term *combat* is used in relation to addressing diseases, it is essential to recognize that it is not akin to a war zone. While it acknowledges the challenging nature of the threat and our efforts to confront it, using the word *combat* in this context raises awareness without implying an adversarial approach among individuals. Instead, our collective efforts are directed towards combating infectious diseases. This incentive to collaborate extends the benefits of collaboration to various fields, disciplines, and actors, including the intelligence community, as they work together to support, generate knowledge, and foster collaboration. Consequently, collaborative efforts in combating the spread of contagious diseases address nontraditional threats and expand the scope of national security concerns, prompting a global response. This study highlights the development of the GLASS by the WHO. Could open-source intelligence potentially encompass a database on the technology of information transfer in which the participating countries worldwide collaborate to report surveillance data on bacterial pathogens of humans? What type of intelligence should be considered for a global surveillance system for infectious diseases?

This chapter delved into theoretical reflections on the research question: How does security governance, facilitated by an open-source intelligence technology database, promote a health regime for the surveillance of infectious diseases? The chapter also explored existing published research and the development of theories such as liberal institutionalism, actor network, and securitization, all anchored to the concepts of security governance, regimes, and complex interdependence. A more progressive and comprehensive actor-network approach was adopted as the analytical framework.

Within this context, complex interdependence emphasizes the emergence of transnational actors, whereas regimes establish the rules of engagement and address various subject matters. Ultimately, security governance establishes a system of rules that govern interactions among actors with the collective purpose of responding to nonconventional threats.

Various factors convince nation-states to act to eradicate specific and complex global issues, because infectious diseases transcend national boundaries. A common interest serves as one piece of the puzzle. In contrast, countries prioritize their economy, political system, and citizens. Through a realist paradigm, nation-states serve as significant actors. However, more than a realist perspective is needed to solve the complexities of global threats, such as COVID-19 or the eight bacterial pathogens that infect humans. A common interest and collaborative security measures intertwine in promoting a health regime. Actors in the policy process push relationships beyond political and bureaucratic relations. The collaboration and interconnectedness of multiple channels and actors are paramount in the shared information exchange. How susceptible is this information to falling into wrong hands? Nontraditional threats go beyond vigilance for infectious diseases. For example, through an open-source intelligence database in the surveillance of AMR shown by bacterial pathogens that infect humans, security governance promotes a health regime. Value exists in monitoring the underlying global threat and the threat of diseases beyond infectious and contagious diseases. The resulting norms characterized by the high involvement of actors in the elaboration process led to the "coexistence of different types of norms" (Brousseau, Marzouki, and Méadel 2012, 5) as principles, rules, and procedures, in other words, regimes. For instance, in opening the black box of a health regime, security considerations need to be kept in mind because of outside unconventional threats that connect actors in co-production (collaboration) of information.

Some theorists emphasize the importance of collaborative efforts in promoting a health regime even in the face of heightened threats and concerns of risk taking, political power, and economic imbalances (Bevir 2007; Fontaine 2015; Haas 1980; Keohane 1984; Puchala and Hopkins 1982; Ruggie 1975). On the other hand, other authors hold differing views on international regimes (Strange 1983; Waltz 1979), and yet others express mixed feelings about their promotion (Jervis 1982; Krasner 1991). Moreover, these theories and concepts demonstrate interconnectedness. Complex interdependence connects to ANT through loosely structured network organizations (Keohane and Nye 1998). Additionally, complex interdependence intersects with the sociology of technology, considering the rapid spread of interdependence between material and social factors (Star and Ruhleder 1996; Latour 1987). Overall, these interconnected theories and concepts provide a comprehensive framework for understanding the dynamics of collaborative efforts in addressing global health challenges.

In turn, the sociology of technology links to regimes where co-production provides more clarity in the social order, such as international regimes (Jasanoff 2004). Regimes connect with complex interdependence by exploring regime analysis and focusing on relationships between interdependence and institutions (Young 1982; Keohane and Nye 2012, 1987), which treats regimes as an interdependent arrangement (Ruggie 1975) and a movement toward complex interdependence (Krasner 1982). Regimes link to the liberal institutionalism theory because health regimes serve as institutions (Keohane 1988). Regimes also extend the scope of institutions (Stein 2008) and connect to complex interdependence because a complex world increases the number of institutions (Coate, Griffin, and Elliott-Gower 2017; Keohane and Nye 2012). Lastly, security governance links to liberal institutionalism owing to institutional capacity as a regulation system in which institutions manage common interests (Bevir 2007; Pierre and Peters 2005). Security governance also connects to the securitization theory, which provides a causal connection between securitization and security governance (Oliveira 2017). Neither theory serves better than the other: the ideas collectively intertwine in developing regimes in the modern complex world, such as the Gordian knot. Neither school of thought influences more than the other but the two are interwoven and provide a wealth of theoretical discourse. The theoretical web develops regimes in such a complex world. Analysis, expansion, and exploration of these thoughts are dealt with in the following chapters.

Chapter 2
Methodology: The Approach and the Means

> Data! data! data! . . . I can't make bricks without clay.
>
> —Sherlock Holmes

As discussed in chapter 1, this study aims to explore how collaboration and interconnection among networks of relevant experts and knowledge production contribute to the establishment of surveillance networks for infectious diseases. The study is driven by three objectives: first, to open the black box of a health regime; second, to analyze the formation of a health regime through security governance in response to an unconventional threat; and third, to elucidate the exchange of open data, the risks associated with it, vulnerabilities, and resources within the utilization of GLASS, and its contribution to the construction of a global health regime, with focus on AMR and the inclusion of COVID-19.

The central research question that guides this study is this: Why did security governance, through the OSINT database of the WHO, promote the health regime on the surveillance of communicable diseases in the northern and southern subcontinent of the Americas from 2015 to 2021? This chapter consists of three sections. The first section discusses the research design methodology, the second section highlights the methodological limitations of the study, and the third section outlines the process of collecting both quantitative and qualitative data and the structuring of those data.

This chapter explains in detail the data collection procedure, which involved a six-step process: 1) determining the level of analysis, 2) identifying actors within the primary unit of research, 3) identifying actors in the network beyond the primary unit that are crucial to the investigation,

4) establishing connections between the actors in the network, 5) mapping the network and creating visual representations of those interconnections, and 6) conducting triangulation. Phase 1, involving quantitative data structure, encompassed steps one to five; phase 2, involving qualitative data structure, comprised step 6.

Research Design

The underlying research philosophy of this study is rooted in positivism. Positivist epistemology was chosen because it emphasizes scientific methods that provide factual evidence and support the claims of legitimate knowledge. In this study, reality was viewed objectively, considering observable evidence as the primary means to defend scientific results. Hence, an objective ontology was adopted, recognizing that there exists only one reality independent of the observer. The study also employed deductive research, starting with established theories and using collected data to further develop and validate them. As a result, a confirmatory approach was incorporated into the study's methodology.

Methodological Approach

This study employs a mixed-methods approach, specifically using explanatory sequential methods to confirm the theories, map the network, determine collaboration among actors, and analyze interconnectedness. This approach was chosen to align with the research objectives, as it allows for a structured investigation of the research questions. The first phase involved quantitative data collection and analysis to identify overarching patterns and relationships. The second phase used qualitative methods to delve deeper into these findings, providing context and a nuanced understanding. This sequential integration ensured a comprehensive exploration of the study's focus areas.

The explanatory sequential design combines quantitative and qualitative methods to map the network and learn about collaborative performance and interconnectedness (Creswell 2014). The design made it possible to follow up the quantitative results with qualitative data to interpret, analyze, and reinforce the information. The core research question focused on *why*; that is, the motivation of the actors behind the actions in the collaborative network. What factors necessitate the outcomes in the surveillance of infectious diseases? Combining quantitative and qualitative data analysis enables a comprehensive understanding of these questions, providing a detailed narrative of the collaboration among diverse actors in response to nonconventional threats like infectious diseases.

Based on the study's aims, the research strategy incorporated four action plans: network analysis, mixed methods, a case-study model, and data and research-gathering tools. The network analysis approach possesses mathematical and visual properties that generate knowledge about relational data. This approach helps to explain and understand how diverse actors interconnect with a common interest. Networks define a structure through patterns of relations between agents and "help to create interests, share identities, and promote shared norms and values" (Knoke and Yang 2008, 6; Hafner-Burton, Kahler, and Montgomery 2009). Networks represent nodes and ties, which illustrate interconnectedness. Networks are coupled with qualitative analysis in the mixed-methods methodology to build a grounded theoretical understanding of actor networks in the surveillance of infectious diseases. Likewise, the intrinsic case-study model suggested by Robert E. Stake (1995) was employed. A case study provides a deeper analysis of the interaction between actors and allows researchers to establish causal relationships with potential theoretical significance (Stake 1995). The study explores the difficulties of tackling a global health issue, the surveillance mechanisms, and the interaction of actors to address, develop, research, prepare, and respond to a global crisis. The study also examines the open exchange of information between actors with a common interest, a collective purpose, and potential security concerns in the mix of complexity. Therefore, there is an intrinsic interest in the WHO-GLASS case.

The time horizon of the study was longitudinal, with data collected at multiple points in time. The data collection focused on the 2015 to 2021 timeframe. Occasional discussions of events outside this period provide research context or illustrate the effects of these occurrences. However, the primary emphasis is on 2015 to 2021 because that period encompassed the early implementation phase of the GLASS initiative, the first global collaborative effort on AMR surveillance standardizing collection and data sharing. Although COVID-19 emerged outside the scope of the selected GLASS pathogens, it serves as contextual evidence and as a reinforcement mechanism for this research study. Therefore, the methodology sought to inspire analysis, analyze networks, and reflect on interconnectedness in the surveillance of infectious diseases such as the AMR of bacterial pathogens affecting humans and COVID-19.

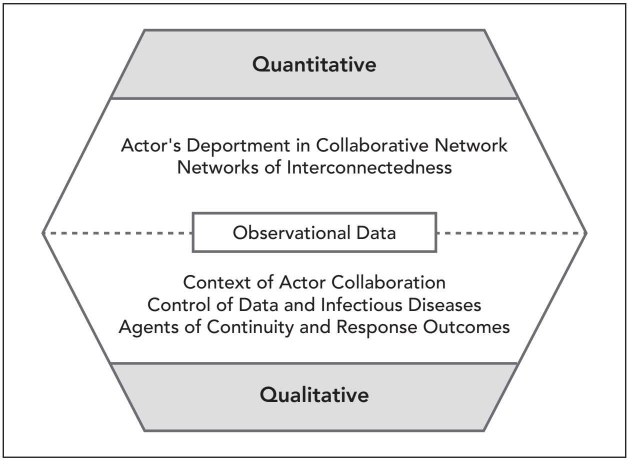
Analysis Techniques

To analyze the collected data, this study employs thematic analysis for qualitative interviews and network analysis for quantitative datasets. These analytical methods were chosen to align with the study's focus on actor relationships and information exchange.

The research relied on three data-gathering tools to collect the necessary data: semi-structured interviews, document analysis, and framework analysis. These tools further facilitate the case-study methodology, a "specific strategy of inquiry," during the qualitative research (Creswell 2014, 176). Descriptive statistics were employed to code the data in the quantitative study, whereas content analysis was used to understand the qualitative study. Information was extracted from Gephi, an open-source network analysis statistical software, for analysis, visualization, and exploration to illustrate networks of interconnectedness (Bastian, Heymann, and Jacomy 2009). Prior to conducting the quantitative analysis, some initial preparation was required, such as removing duplicates in the Excel and .csv files. Network visualization serves to reveal patterns and trends, highlight outliers, and tell the story of interconnectedness and collaboration among actors.

Moreover, this investigation incorporates a framework method to support qualitative content. Drawing on the information in the explanatory sequential design model described above, figure 2.1 represents the research undertaken in this study.

Figure 2.1. Research framework



The two elements above the dotted line represent the quantitative data structure analysis, which includes the network analysis and content analysis approaches to explain the material that underpins collaboration and interconnectedness in security governance. This study examines these two elements in greater detail in phase 1 of the data analysis in chapter 3. The three elements below the dotted line represent the analysis of the qualitative data structure. The analysis of these three elements is conducted in phase 2 of the data analysis in chapter 3. In figure 2.1, observational data are placed in the middle of the research framework because they are used in both phases. Through the specific case study in chapter 3, the research examines the context and control elements in greater detail. Lastly, this study addresses the element of continuity and response outcomes in chapter 4.

Data Collection Method

This study utilized a combination of quantitative and qualitative data collection methods to gather comprehensive and actionable insights. Quantitative data were collected through statistical datasets, while qualitative data were obtained through semi-structured interviews and document analysis.

These methods were carefully chosen to complement each other, providing both breadth and depth to the research. For a detailed description of the data collection process, including specific instruments, strategies, and data sources, refer to the following data collection. This subsequent section elaborates on the procedural and practical aspects of gathering the data, ensuring transparency and methodological rigor.

Data Collection

In this section, we will examine the tools and processes used for data collection to ensure alignment with the research objectives. This includes the quantitative and qualitative data collection methodology to provide a robust foundation for the subsequent analysis.

There is nothing natural about emergencies and disasters during a pandemic that brings about stress. Which actors either interconnect or limit the network while conforming to a system of rules to fight nonconventional threats to promote a health regime? This section describes the collection of data for both quantitative and qualitative data structures. The research includes a mixed-methods approach to the analysis. The first stage of the data collection and analysis process commences with the quantitative data structure to establish interconnectedness and collaboration between actors to establish a causal relationship between security governance and the emergence of a health regime. The research measures the variables to map the network and analyze interconnectedness by creating the graphs and networks through Gephi, a software program (Bastian, Heymann, and Jacomy 2009), and incorporates aggregated sources of macro data from the GLASS platform and official reports. Gephi facilitates network analysis and data visualization. Moreover, the software reinforces diverse collaborating actors (nodes) such as infectious diseases, the GLASS database, and the IHR as boundary objects in the network.

Through the network analysis approach, this study also incorporates content analysis, which includes observational data to obtain deeper insights. For example, infectious diseases and pandemics affect emergency control, disaster readiness, economic turmoil, and international relations. For Knoke and Kuklinski (1982, 21), the "choice of methods for locating positions in an empirical network ultimately depends … on the substantive and theoretical problem the analyst is addressing." This study traces the actors using the ANT inspired by Latour's (2005) advice to go slow, not jump, and keep everything flat. The theory (ANT) has illuminated the limitations of the network, enabling a more focused examination of the data. This involves sifting through the information gathered from various actors and pinpointing relevant positions within the network. Thus, to discover the breadth of the task on hand–to separate the relevant actors from the irrelevant ones–is to slow down, review the collection, analyze the information, and sort the data.

The procedure to structure quantitative data identified the actors in the network, drawing on relevant information from the GLASS platform and the actors interconnected with it. Data from the following sources were collected and analyzed, primarily using GLASS through the WHO and, as a secondary source, the ReLAVRA through the Pan American Health Organization (PAHO). A network is a relational link between objects, persons, or events (Knoke and Kuklinski 1982; Mitchell 1969). Three elements, namely, sampling units, relational form and content, and the level of data analysis (Knoke and Yang 2008; Knoke and Kuklinski 1982), inspire the creation of the actor-network research design and quantitative data structure. The procedure entails five steps: choosing a level of analysis; tracking and sorting the GLASS-participating countries with a common interest; identifying third-party actors with high visibility related to the network drawn from primary sources; identifying and linking the network actors based on interconnectedness, collaboration, and relation to the security threat; and the visualization and statistical analysis of actor interconnectedness. The following section discusses the data collection methodology. Chapter 3 describes the process of data analysis and interprets the results of the analysis through a specific case study.

Phase 1: Quantitative Data Collection Methodology

This study aims to address issues in network observation related to the fundamental problems of specifying the network boundary and resolving the entities or actors that make up the network. A methodological contribution is made to the empirical investigation of actor collaboration and interconnectedness, seeking to advance a paradigm shift in network methods toward a progressive movement to identify network actors. The proposed approach includes a five-step procedure that combines content analysis with observational data and framework analysis of hierarchical data collection. In this procedure, the analyst undertakes the following tasks:

1. Choosing a level for the analysis (macro, meso, or micro). Having a focal point early on in the investigation allows the analyst to select the relevant actors.
2. Identifying the actors within the primary unit of investigation. This research extracts actors linked to the primary locus. At this stage, the task includes subjective choices of actors depending on the data structure.
3. Identifying the actors relating to the network drawn from sources outside the primary unit but considered fundamental to the research. This large pool of candidates enlarges the scope but removes the collection limits derived from the first procedure to create the network of interconnectedness.
4. Linking the actors in the network based on their relation and interconnectedness to the object of a security threat. Essential to the network, this action focuses on collaboration (compliance or resistance) to address the security threat.
5. Showcasing a visual representation of actor interconnectedness. Appropriate graphics help readers comprehend the information revealed from the investigation.

Step 1. Three Paths: At the Crossroads of Macro, Meso, and Micro

In step one, the researcher chooses one of the three paths or a combination of the three levels of analysis: macro, meso, or micro. This initial step is crucial in the investigatory process because it provides a focal point and simplifies the sorting of actor data within the network. At the macro level, institutions and large-scale patterns of actors affected by national security threats, such as infectious diseases, are examined. The meso level focuses on analyzing the arrangement of security governance and the interconnectedness of like-minded actor groups in the surveillance of infectious diseases, with the aim of promoting a health regime. It is important to note that the meso level of analysis acknowledges both the macro and micro levels. However, this study does not delve into micro level analysis, which involves examining individual interactions such as those between doctors and patients or specific health care practices related to diagnosing and curing infectious diseases.

The investigation aims to measure how actors conceive a system of rules, known as security governance, in response to security threats. The focus is on understanding how various agents, including international organizations, NGOs, and private interest groups, implement security governance in nontraditional security areas. The analysis also explores whether other actors, such as policymakers, military personnel, teams dealing with hazards, and medical emergency teams, provide real-time responses in the collaborative process to mitigate strategic surprises. Additionally, the study examines how governments collaborate with private actors to address infectious diseases while considering security measures. By adopting a macro- and meso-level inquiry, the analysis can concentrate on specific actors to create the network and explore their interconnectedness.

Step 2. Unit of Investigation: Tracking and Sorting Actors

In step two, following the selection of the research level, the analyst proceeds to identify pertinent actors within the primary unit of analysis associated with the chosen focal point to design the network. The present study extracts relevant actors that are connected to the focal point during the data collection and network design phase. In this process, the analyst includes an arbitrary selection of actors based on the data structure. The focus of this research is on the analysis of the GLASS platform. Consequently, actors such as participating countries and nonhuman entities such as the GLASS platform, the IHR, and infectious diseases linked to the technology database are extracted to compile the network.

Step 3. High Visibility: Third-Party Actors and Primary Source Extraction

In the third step, actors that are relevant to the investigation but originate from sources outside the primary analysis unit are identified. This study uses a variety of sources, including interviews, official news outlets, observable actors, governmental events and meetings, and official documents such as epidemiological situation reports (SITREPs), Congressional hearing reports, White House briefings, and reports from government departments responsible for health-related matters. The selection of third-party actors for inclusion in the data collection is based on the recognition of "the need for ongoing vigilance against the onset of an event that has never before occurred," which is one of the fundamental premises of global health security (Lakoff 2015, 315). While there are numerous actors and potential samples to consider, this study focuses on formal groups, individuals at an executive level, and organizations as sampling units. This specific category of actors forms a significant portion of the research inquiry, as it lies within the scope of a macro- and meso-level investigation. Therefore, this pool of candidates represents a targeted selection that contributes to the creation of the network of interconnectedness but excludes the broader range of actors collected in the first step.

Step 4. Network Linkage: Global Relations and Collaboration

The fourth step involves establishing connections and relationships among actors based on their interconnectedness and their willingness or unwillingness to collaborate in addressing the security threat. In other words, the identification of actors in the network under investigation is based on their interconnected relationships with other key actors. In this study, actors are considered to be collaborating if they engage in substantial communication such as exchanging information or submitting surveillance data in accordance with a set of rules pertaining to task performance. As the direction of collaboration or interaction among actors, based on document review, was not consistently apparent, collaboration was coded as an undirected network. Similarly, no distinction was made between different types or levels of collaboration, as the documents did not fully specify the collaborative nature of the relationships. The interconnection aspect highlights the relational dimension of the network as a crucial element. Consequently, this study presents collaboration as a dyadic relation involving discretionary actors.

Step 5. Interconnectedness: Visual Representation

The fifth step involves the visualization of actor interconnectedness. In this study, the newly collected data and information were analyzed, transferred, and fed into the Gephi software. Descriptive statistics were then used to analyze the compiled data statistically. Finally, this process generates an infographic that captures and presents the visual and statistical analysis of actor interconnectedness. The visual element serves to complement the text, enhance clarity, and assist readers in comprehending the subject matter.

Phase 2: Qualitative Data Collection Methodology

This section focuses on the qualitative data structure methodology, and chapter 3 provides an in-depth exploration of the data analysis and results. The qualitative structure primarily relies on semi-structured interviews and documentary analysis as data-gathering tools. The sources of data were collected manually from a corpus of online documents spanning from 2015 to 2021. A range of public and official government documents were analyzed, supplemented by general research using the internet, library visits, observations, and institutional visits. The case study employed both quantitative and qualitative approaches using various data-gathering tools.

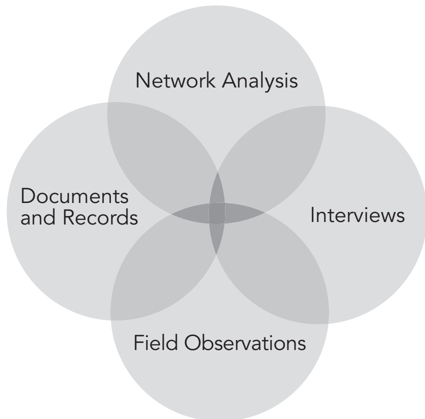
Fieldwork was conducted in the United States, and the data collection process included interviews, general internet research, and document review from diverse primary sources and publicly available information.

Semi-structured interviews were conducted with a variety of primary sources, including government officials, NGOs, academics, and experts in health, military, security, intelligence, and software development. Each interviewee offered unique experiences and insights. Data analysis was conducted by collecting information from the GLASS developed by the WHO. Document analysis, semi-structured interviews, and framework analysis were employed as data-gathering tools to analyze the context of collaborative actors, the actors' control of diseases and data during open information exchange, and the types of responders acting as agents of continuity in the surveillance of infectious diseases.

The section on data collection processes expands the five-step procedure outlined in phase 1 of the quantitative data structure. In phase 2, the qualitative data structure incorporates triangulation, which represents the sixth step in the procedure. Triangulation involves analyzing interview data alongside information gathered from other sources. This approach of blending diverse sources enables models to unearth hidden knowledge within vast seas or flowing rivers of data (Pando and Poggi 2020). The qualitative analysis involved reviewing data from documentary sources and observational studies. Additionally, incorporating perceptions of the interviewees provided valuable analytical insights: "observations work the researcher toward greater understanding of the case" (Stake 1995, 60). Therefore, the comprehensive use of various data sources and the analytical depth gained through qualitative analysis contributed to a robust understanding of the subject matter.

Data for this study were gathered from various official sources, including the U.S. Department of Health and Human Services (HHS), the Centers for Disease Control and Prevention (CDC), the PACCARB, reports or Congressional hearings, SITREPs, and other official documents, such as the U.S. government's global health security strategy. This research included participatory analysis or direct observation review (Knoke and Kuklinski 1982). In addition, this study triangulated the data from quantitative analysis of the actor nodes in the collaborative networks with information gathered from semi-structured interviews and documentary analysis. Figure 2.2 illustrates the triangulations used in this research study.

Figure 2.2. Venn diagram of methodological triangulation



In this context, fieldwork for the research reported in this book was conducted to assess instances of collaboration in security governance concerning surveillance for infectious diseases and data control, with the aim of promoting a health regime. An analyzed dataset was created by employing document analysis, comparison of data, and observational methods. Active participation in institutional meetings facilitated the collection of data from observable actors, allowing regular patterns of relations among network nodes to be detected and observed. Subgroups, characterized by the patterns of relations, represented observable behaviors that linked empirical actors (Knoke and Kuklinski 1982). The documents analyzed for this study were selected based on their official nature and they included the following:

- white papers, briefings, and Congressional hearing reports published by the U.S. government (chapters 3, 4, 5)
- unclassified reports and threat assessments from military and intelligence sources (chapters 4, 5)
- health care, infectious diseases, and global health reports (chapters 3, 4, 5)
- epidemiological SITREPs (chapters 3, 4, 5).

Observing and analyzing the practices and actions of actors influences a network's connectivity because knowledge is produced on the usefulness of technology, such as the GLASS database, and how actors collaborate to create greater global awareness of the importance of interconnectedness.

This study reviews and analyzes many relevant open-source materials produced by organizations and actors involved in responding to surveillance for infectious diseases. Infectious diseases pose a unique challenge as they straddle the traditional notions of national security, which primarily focuses on military threats, and the broader realm of threats to public health and well-being. Drawing inspiration from Goffman, this study seeks to minimize potential biases inherent in materials created for external entities by turning to the backstage documents "where the suppressed facts make an appearance" (Goffman 1959, 69). The primary objective is to explore the interconnectedness of various actors, both human and nonhuman, within the security governance of infectious diseases, with the ultimate goal of promoting a robust health regime.

Determining the causality in measuring security governance, specifically the control of diseases and data within the surveillance for infectious diseases, involved analyzing eight selected bacteria with AMR data to identify incidents of threats recognized by member-states on the surveillance platform from 2015 to 2021. A thorough examination was conducted on the GLASS platform and statement reports pertaining to AMR issued by the HHS, which serves as the ministry of health. These reports were essential in understanding how ministerial meetings influenced the perception of pathogens as potential threats. Using publicly available information, an analysis was conducted to examine the frequency of discussions regarding AMR by the HHS from 2015 to 2021. Additionally, the study investigated the stance taken by the HHS on the topic of AMR.

In addition, summary reports of the HHS council were examined to track the frequency of HHS meetings and review resolution statements. Analysis was conducted to determine if any GLASS member-states from the northern and southern subcontinents of the Americas held separate AMR meetings and their voting patterns on related resolutions. Tracking the enactment of laws for safeguards in the database, particularly those established by the ministries of health or by nation-states to implement security measures, formed another aspect of the causal relationship. Furthermore, statements pertaining to national security matters within the scope of this study were reviewed: these offered insights into instances of a causal relationship. Specifically, statements issued by ministries of health were tracked to observe the frequency with which participating member-states in the Americas declared a specific pathogen as a threat. Additionally, an examination was made to ascertain whether the HHS engaged in discussions focused on AMR and whether nation-states or institutions generated regulations concerning global health issues. Lastly, an exploration was conducted to understand how these statements related to the overall landscape of the GLASS.

This study, as detailed in chapter 3, adopts a framework method aligned with a set of themes that underpin qualitative content analysis. The initial phase involved conducting semi-structured interviews aimed at unraveling nuanced facets of the openly constructed phenomenon where the "capacity of a performance to express something beyond itself which may be painstakingly fabricated" (Goffman 1959, 69). Building upon the five-step quantitative data structure, the qualitative data framework introduced an additional sixth step, namely, triangulation, in the procedure. To achieve triangulation, data from semi-structured interviews, analyses of official documents, and observational reviews were harmonized and cross-referenced. By incorporating collaboration among actors involved in surveillance for infectious diseases and security governance, this research sheds light on the intricate dynamics of the security governance process in controlling disease surveillance and facilitating data sharing, ultimately fostering the emergence of a health regime.

This study encompasses a comprehensive collection of diverse research materials, rooted in theories supported by empirical evidence. The acquisition of these materials involved several key steps. Firstly, university and public research libraries were accessed to gather relevant sources. Secondly, a meticulous manual search was conducted across various online platforms, targeting documents related to the GLASS and AMR responses spanning the period 2015-2021. The identification of sources was accomplished through a range of methods, including the utilization of commercial search engines such as Google, direct browsing of federal and state websites, and a thorough review of other organizational websites deemed relevant in terms of their potential contribution to continuity in the field. This systematic process was consistently applied throughout the data collection timeframe, allowing for the retrieval and subsequent manual review of the identified materials.

The collected documents encompassed a wide array of sources, including SITREPs, maps, Congressional hearing reports, White House briefings and statements, infectious disease response reports, and various other official materials sourced from entities such as the HHS and the CDC. Table 2.1 provides an overview of the source institutions categorized by type. The compilation comprises approximately 1,500 documents obtained from 21 different source institutions. Notably, the documentary data derived from government sources encompass both federal and state governments. The agencies category included regulatory bodies, security organizations, emergency management agencies, and ministries of health, while the organizations category encompassed intergovernmental entities, non-profits, NGOs, and other relevant actors.

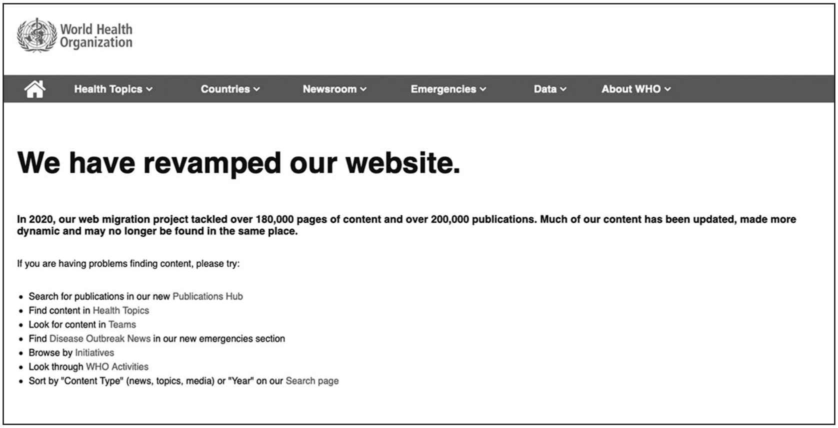
During the data collection, it was observed that websites underwent frequent reorganization of information. For instance, in 2020, the WHO revamped its website as part of content updates and a web migration project, as depicted in figure 2.3.

Although such highly specialized automated information search and retrieval browsing services as Argos, Spider, MathSearch, NEC-MeshExplorer, and Social Science Information Gateway (SOSIG) help to locate new information (Kobayashi and Takeda 2000); however, manual searches have an advantage over automated browsing services, such as the crawlers mentioned

Table 2.1. Source institutions, by type

Type of source institution	Count
Governments	8
Agencies	8
Organizations	5
Total	**21**

Figure 2.3. Example of problems with the original source website



Source: World Health Organization (2020).

earlier or intelligent agents (Kobayashi and Takeda 2000) in that the latter may not capture misspelling of URLs or organizations that change the information and its location on the website. Thus, to adequately retrieve and document all relevant data, it was imperative to conduct a manual review and ensure the retrieval of correct and up-to-date information.

In addition, a case study method incorporating semi-structured interviews with individuals from diverse fields relevant to international studies was used. The interviewees included government officials, academics, staff of the relevant institutions and NGOs, and experts in health care, security, intelligence, and military matters. This approach ensured a comprehensive perspective by engaging individuals with well-established positions within their respective communities. The study revisited phase 1 of the quantitative data structure to extract information about relevant actors to conduct the interviews for the second phase of the qualitative data structure. During phase 1, four distinct CNPs and visualization designs were created. As a tool, networks represent a pair of relationships in physical or social systems, which can be used as an abstraction for studying the interconnection between components (Feng and Kirkley 2020). The research process involved reviewing the GLASS platform, the pathogens, and information from AMR surveillance provided by participating member-states. The focus was on understanding how participating countries interconnect and collaborate in the exchange of open data.

In this instance, global collaboration improved the understanding of AMR and informed "containment and mitigation strategies" of infectious diseases (World Health Organization 2017b, 5). Three types of information drive a source of collaboration: information commercially provided at a price, valuable strategic information that is contained lest it should fall into the wrong hands, and free information that actors create without compensation (Keohane and Nye 2012). In addition, data availability empowers emerging technologies such as AI, algorithms, and high-performance computing. After analyzing the networks, an examination of the categories with the highest and lowest degrees of collaboration was conducted, inspired by the third type of information driver, namely, free exchange of information between actors. This analysis helped to identify key categories for further investigation. Subsequently, semi-structured interviews were conducted with diverse sources, ensuring full anonymity of the interviewees.

A compact list of thematic and issue-oriented questions was developed, focusing on topics relevant to the research question and objectives of the study. These questions were designed to gather descriptions of concepts, events, connections, links, understanding, and explanations from the interviewees. The insights and responses provided by the interviewees during the fieldwork were then analyzed to support the core research question. The semi-structured interview format encouraged the interviewees to delve deeper into their thoughts. For example, an interviewee with expertise in policy and technology emphasized the balancing act between surveillance mechanisms and information rights of the individual, particularly regarding powerful computers and the control of information dissemination. Conversely, an expert in health and security stressed the significance of trust and reliable actors in fostering collaboration. This interviewee emphasized the importance of avoiding excessive securitization and recognized that although securitization often relies on proprietary means, not everything should be subjected to such measures.

Topics explored during the interview process encompassed a range of critical aspects, including the perspectives of actors on threats to national security, the significance of securitization in certain domains, concerns related to bias in algorithms, privacy issues surrounding data sharing, and the importance of regulatory frameworks, among other subjects relevant to the research. These interviews served as a valuable source of additional insights and provided further guidance for the study. A total of 14 experts were interviewed, and their interviews were transcribed and organized into distinct categories based on the identified themes. The selection of these 14 voluntary participants was based on the 16 actor-type categories outlined in the quantitative data structure. These actor category types encompass a diverse range, including academia, contextual groups, countries, funders, teams dealing with hazards, individuals, institutions, intelligence agencies, law enforcement agencies, medical emergency teams, military personnel, nonhuman actors, policymakers, researchers, scientists, and security-related entities. Using this categorization, an initial blueprint was drafted, serving as a foundation for further analysis and discussion, and was segmented into five categories based on the interviewees' practices within the collaborative network (table 2.2).

As the interviews and data collection progressed, the themes in table 2.2 were expanded, and the interviewees were grouped into seven distinct groups within the 16 categories. This categorization allowed for a more comprehensive analysis and understanding of the data collected from the interviews. Some interviewees possessed expertise in multiple fields, resulting in their inclusion in two to three categories. An overview of the

Table 2.2. Baseline descriptive actor participants in the collaborative network, by practice

Academic	Healthcare	Intelligence	Security		Military
			General	Cybersecurity	
• Professors	• Ministry of Health • Medical Officer • Epidemiologist	• Department of Defense • Technology and Policy Expert	• Security and Information Technology Executive	• Communications • IT Department • Cybersecurity Expert	• Branch of U.S. Armed Forces

distribution of interviewees across the categories is presented in table 2.3. Out of the 16 categories, 14 interviewees were allocated to seven categories, namely, academic, NGO, health care institution, intelligence, military, researchers, and security, whereas the remaining nine categories did not have any interviewees. The interviewees encompassed a diverse range of roles, including medical officers from the WHO, AMR lead executives from the WHO, officers from an NGO, special operations military executives, military officials, military officers from the Department of Defense, officers from the CDC, a medical doctor and advisor from PAHO, professors in academia, and an intelligence consultant in sustainable development.

The interviews were conducted during 2019-2020, employing various modes such as the telephone, in-person, and email. The initial interview questions were designed to explore specific keywords related to the study's subject matter of health and security. These keywords included surveillance systems, open-source, security governance, regulations, GLASS, private and public actors, interconnection, collaboration, national security, and dissident groups. The interviews were initiated with specific questions, but the conversation was allowed to develop naturally, enabling a deeper exploration of the research topic. This approach facilitated the discovery of new insights and perspectives while maintaining focus on the main research question.

The selection of these interviewees was based on their expertise in fields relevant to health, security, science, and technology within the scope of

Table 2.3. Distribution of interviewees, by category

Category	Interviewees by category	No. of interviewees
Academic	2	2
NGO	2	2
Healthcare institution	5	5
Intelligence	1	1
Military	3	3
Security	3	1
Researchers	2	0
Total		**14**

AMR, the primary subject matter of this book. However, the ongoing global pandemic posed limitations on conducting additional interviews. The limitations of this practice are further elaborated in chapter 5.

The data collection consisted of interviews with stakeholders in health and security in the private and public sectors and experts in the field, including local, national, and international government and non-government officials. Based on the analysis of the network from the quantitative data structure, specific actors from the different categories were interviewed to obtain data for the qualitative data structure phase.

This chapter presents the blueprint for empirical research that was part of the study aimed at answering the research question. The first section provides an understanding of the research design methodology; the second section discusses the methodological limitations of using a mixed-method approach in this study; and the third section focuses on the data collection process, including phase 1 of the quantitative data structure and phase 2 of the study's qualitative data structure.

Networks provide a valuable means of acquiring knowledge by leveraging existing information. Although a quantitative analysis through network analysis provides valuable insights, it is important to complement that analysis with qualitative analysis. Qualitative analysis helps to reinforce the statistical aspects gained during network analysis by delving deeper into the contextual and subjective dimensions of the data. By combining quantitative and qualitative information, experts and researchers gain a clearer and deeper understanding of the complete story. Furthermore, mixed methods allow a broad range of thought, analysis, and results. By means of an intuitive approach to research, individuals, multiple disciplines, and diverse industries have used mixed methods in their everyday lives. Thus, the process allows the collection, combination, and integration of data collected from multiple sources.

Mixed-method research offers a comprehensive understanding of the research problem, but it also presents limitations that must be acknowledged. Managing time, generalizing data, and analyzing data from two different data points can be challenging. Moreover, when integrating the results of both datasets, the data can be transformed, and conflicting results between qualitative and quantitative data can challenge the validity and interpretation of the evidence. The imbalance in data representation is a disadvantage that can hinder the interpretation of results from the analysis of data. Therefore, researchers using the mixed-method research design must consider these limitations and develop strategies to address them.

Nonetheless, the approach allows the investigator to balance out the limitations because mixed methods provide a richer source of information, clarity in knowledge production, and an amalgamation of content. The triangulation of information allows for expansion and development of the study. A quantitative data structure gives the study an air of dry and technical objectivity whereas interviewing and triangulation of documents within the qualitative data structure bring the technical aspect down to a more holistic but subjective level. By combining qualitative and quantitative research, this study obtained a deeper and comprehensive understanding of the phenomenon under investigation, specifically the emergence of a health regime in the surveillance for infectious diseases and AMR.

This study used the mixed-methods approach to identify actors in the network and their interconnectedness. The quantitative research method allows multiple actors to connect to the primary unit of analysis and other relevant actors with as much common interest in the boundary object. This study created a four-actor-network graphic to help visualize the techniques for network analysis, detailed in the data analysis section of chapter 3. These distinct paths of interconnectedness illustrate the roles of surveillance and collaboration in combating infectious diseases. The design also showcases contextual information on the actors disassociated from the network but integral to network analysis.

The research shows that a network comprising diverse key actors who interconnect and exchange ideas and knowledge across different disciplines can drive information exchange and knowledge production and shape various industries in terms of science and security. By adopting a network analysis perspective that considers the overall structure of actor relations, a foundation can be established to develop the dimensions of security governance described in the next chapter. The integration of quantitative and qualitative analysis through a mixed-method approach provided valuable scientific support.

The ideas discussed in this study have far-reaching implications that extend to diverse fields and disciplines. The methodology used in this research holds the potential to make substantial contributions to areas such as intelligence, security, and strategic studies. Furthermore, it can provide valuable insights for military operations, efforts to reduce the risk of disasters, and strategic management practices. Using network analysis, researchers can study groups, people, and their interactions, which can help military, security, and intelligence analysts identify significant threats and relevant actors connected or linked to the threat. This analysis can also help decision-makers and stakeholders to identify actors to collaborate and engage with an organization such as the WHO. Disaster management specialists can use relevant methodological data to identify appropriate actors in an organizational network to assist the organization in tackling and minimizing risks from those disasters. Although mapping an actor-network creates a practically endless and exhaustive list, knowing key players in the network gives a head start to organizing, knowing what to do, and collaborating with others when disasters or emergencies strike.

The next chapter offers a deeper examination of the case study of the WHO-GLASS for AMR. The chapter starts by establishing a framework for security governance metrics, providing guidance for analyzing the data and deriving significant insights. Next, the results of the data analysis and collection are presented, revealing various aspects of the collaborative network. Additionally, the chapter focuses on countries in the northern and southern subcontinents of the Americas. The analysis aims to reinforce the map of the collaborative network formed to deal with surveillance of infectious diseases, evaluating how well collaborative actors perform, and understanding the nature of their interconnectedness. By exploring these aspects in detail, we aim to gain a deeper understanding of the dynamics of the collaborative network and its implications for global health security. The chapter contributes valuable insights to our overall research objective of comprehending the complexities of global interconnectedness in addressing emerging health threats.

Limitations of the Methodology

One limitation of the study is the deliberate focus on a specific case study, which restricted the exploration of other curiosities and interests. However, the more we set aside curiosities for other similar case studies, "the more we will try to discern and pursue issues critical to the case study" (Stake 1995, 4). By concentrating on a single case study, the study benefits from particularization rather than generalization (Stake 1995). This approach allows for a comprehensive understanding and analysis of the case study, including its intricacies, uniqueness, and knowledge production. Consequently, by delving deeper into the curiosities specific to the case study, the emphasis is on understanding the case study itself.

This research includes insights from confidential sources to provide nuanced perspectives on topics where public documentation is limited or nonexistent. Confidential interviews were conducted with individuals directly involved in relevant areas, including cybersecurity and public health governance, ensuring their relevance and expertise. To maintain academic rigor, the validity of these sources was cross-verified with publicly available data and corroborated through triangulation with other interviews and secondary data. The assurance of confidentiality was critical to obtaining candid insights, a standard practice in research involving sensitive or security-related topics.

Another limitation is that the research was limited solely to using quantitative and qualitative approaches, which meant that its outcomes depended only on that method. Although there is nothing wrong with using just one method, this approach may result in insufficient information. Furthermore, using quantitative research alone makes for deficiency in the tone of the voice of the research subject and the experience accumulated by the researcher. "When researchers quantitatively examine many individuals, the understanding of any one individual is diminished" (Creswell and Plano 2018, 8). Likewise, quantitative methods–although valuable in demonstrating correlation between variables–fail to reveal whether that relationship is causative (Lamont 2015; Denzin and Lincoln 2008), which may make the results of data analysis potentially misleading

(Mertens et al. 2016). Therefore, quantitative research alone amounts to being more impersonal and suppresses the voice of the participants.

On the other hand, qualitative research provides only indirect and soft data, unlike the complex data supplied by quantitative methods. Studying quantitative data collection or fewer subjects results in generalized confusion (Creswell and Plano 2018), lack of structure and consistency (Lamont 2015), and unmeasured quality of the entities (Denzin and Lincoln 2008). Although analysts can translate qualitative data into quantitative information, Kitchin (2014) noted that the transition involves a significant reduction and loss of richness in the original data, whereas Denzin and Lincoln (2008) added that the integrity of statements relies on quantitative facts. Therefore, researchers need to reinforce the information with numbers to verify the truthfulness of the qualitative statements. Thus, without a large enough pool of subjects, relying on only a small number of participants limits the researcher's experience and the outcome of the research.

Added to the limitation of mixed methods was the arduous task of managing time. This study faced several challenges in using a mixed-methods approach, and the explanatory sequential design had a few drawbacks in the investigatory process during the COVID-19 pandemic. Much time was spent on receiving, sorting, and analyzing massive amounts of information in two separate phases (Creswell 2014). The study aimed to divide the time between obtaining quantitative and qualitative data and analyzing the programmed schedule. However, as time was of the essence, it took a great deal of work to organize the research within the constraints imposed by time. Thus, the mixed-methods approach presents challenges in obtaining the data when researching for a limited period, making it necessary to divide the time between quantitative and qualitative collections, coupled with a global pandemic.

Furthermore, the use of mixed methods in research presents challenges to the researcher in terms of designing the overall study and managing time when employing both types of methods simultaneously. It is also common for researchers to develop a stronger interest, or to gain more experience, or to acquire greater skills set in one specific method over the course of research. In this study, the emphasis was initially on quantitative data structure owing to its ability to generate concrete insights based on statistical analysis. However, an unexpected fascination with network analysis emerged, highlighting the need to allocate equal attention to qualitative data structure. Ultimately, the project leaned more toward quantitative analysis in terms of passion and focus, while recognizing the significance of both methodologies.

However, the emphasis shifted towards the qualitative structure upon recognizing the imbalanced focus within the constrained timeframe. Maintaining an analytical equilibrium becomes crucial in conducting mixed-methods research, which is why researchers should allocate equal time and effort to both quantitative and qualitative analysis. In contrast, the use of mixed-methods research in the field of international studies offers a comprehensive perspective by elucidating social phenomena through data-driven statistics and interpreting the humanistic reality of the social world.

Employing a combination of qualitative and quantitative data through mixed-methods research enhances the value of generating a holistic view and fostering deeper comprehension of the research question. Creswell and Plano (2018, 12) suggest that the "strengths of one approach make up for the weaknesses of the other." This method gathers well-rounded information and enhances complementarity and triangulation. Mixed methods provide a more comprehensive collection and analysis of data. Furthermore, combining both approaches allows the investigator to obtain greater knowledge of the unit of analysis. Therefore, this research opted for the mixed-methods approach because it opens the possibility of yielding diverse outcomes in the study.

The mixed-methods approach is increasingly used by many and different industries. "Mixing methods is an intuitive way of doing research that is constantly being displayed throughout our everyday lives" (Creswell and Plano 2018, 1). For example, in the media industry, a broadcasting network relies on Nielsen ratings to develop its programming lineup. The network utilizes Nielsen statistics to analyze the ratings and make informed decisions. Additionally, the network employs qualitative marketing tools to gain insights into which programs engage and resonate better with its viewership. By incorporating both marketing research and statistical data, the network obtains a comprehensive understanding of its audience and programming dynamics. This integration of mixed methods equips the network to enhance its current programming, secure sponsorships, increase ratings during sweeps periods (time slots in which media companies expect to reach a larger audience through broadcast programming that matches its viewers' likes and interests), and make the necessary adjustments to future programming strategies.

Likewise, law firms rely on such software packages as Capital IQ and Monitor Suite to collect quantitative data for company profiling and competitive intelligence reporting. These tools provide law firms with valuable quantitative information. The firms supplement these data with qualitative research methods, such as organizing client outreach events and making follow-up calls, to generate more business development opportunities. This real-world scenario exemplifies consistent use of a mixed-methods approach in which both quantitative and qualitative methods are employed to enhance decision-making and achieve comprehensive insights in the legal field.

Mixed-method research blends two types of data collection, combining "at least one qualitative and one quantitative method in the same research project or set of related projects" (Hesse-Biber 2015, xxxix). Over time, the definition of mixed methods has evolved to encompass more nuanced methodologies. Creswell and Plano (2018, 5) describe this approach as follows:

> [The researcher] collects and analyzes both qualitative and quantitative data rigorously in response to research questions and hypotheses; integrates … the two forms of data and their results; organizes these procedures into specific research designs that provide the logic and procedures for conducting the study; and frames these procedures within theory and philosophy.

On the one hand, qualitative methods provide a "detailed understanding of a problem" and a particularized canvas by looking beyond the numerical scope by reflecting with open-ended questions when analyzing the meanings of a text, image analysis, and interviews (Creswell and Plano 2018, 8). On the other hand, quantitative methods provide a general understanding, a bigger picture on the surface based on statistical analysis and quantify facts by comparing scientific data and variables. While either approach alone passes muster, mixed methods are considered "applicable to a wide variety of disciplines in the social, behavioral, and health sciences" (Creswell and Plano 2018, 7).

Also, triangulation and complementarity are two ways to design mixed-methods research that adds value to the study results (Lamont 2015). According to Sanclemente (2018), recent scholars such as Lamont (2015) attributed complementarity to large-N quantitative work complemented with a small-N study and triangulation as corroborating the findings of an investigation. The "combination of quantitative and qualitative data provides a more complete understanding of the research problem than either approach by itself" (Creswell and Plano 2018, 8). Nonetheless, neither approach stands to be more valuable than the other. For this study, the mixed-methods approach offers a comprehensive perspective of the interdisciplinary approach, encompassing the social sciences, including international studies, law and policy, and science and technology disciplines.

Moreover, there are three strategic designs a researcher chooses within the mixed-method research. The explanatory sequential strategy involves depending heavily on quantitative data in the first phase, followed by qualitative data. The sequential exploratory strategy, on the other hand, begins with qualitative data collection in the first phase, followed by quantitative data collection. Lastly, the mixed-methods convergent design involves using both the strategies concurrently: the researcher collects both qualitative and quantitative data in one phase to determine if the analysis results are convergent (Creswell 2014). Therefore, as indicated earlier, the study used the explanatory sequential design to map the network and determine the extent of collaboration among actors and their interconnectedness.

Employing the mixed-methods research presents challenges when factors such as time, space, lack of training, and time management impact the study's outcomes. For instance, when a researcher devotes more time to one method, it may add limited value to the overall study. Therefore, researchers employing mixed-methods research must carefully assess the limitations and constraints that may affect their analysis of data. Nonetheless, using multiple data tools within mixed-methods research offers the advantage of addressing a wider range of research questions. By combining qualitative and quantitative data, mixed-methods research allows for a more comprehensive analysis of the research problem, informing and enhancing the understanding of the research question on hand. Despite its limitations, employing the mixed-methods approach provides a more holistic and complete picture of the phenomenon under study.

Chapter 3
Studying International Relations Quantitatively and Qualitatively

> It is a serious thing just to be alive on this fresh morning in the broken world . . . It could mean something. It could mean everything.
>
> —Mary Oliver

The research presented in this book is structured around a logical (deductive) model aimed at explaining theories grounded in empirical evidence, with a focus on a specific case study. This chapter investigates the five dimensions of security governance within the context of data exchange in an open-source database for infectious disease surveillance, building upon the data collection methods described in chapter 2. The central inquiry examines how actors effectively manage, coordinate, and regulate security governance within a global open-source database. To illustrate these dimensions, the selected case study is the World Health Organization's Global Antimicrobial Resistance Surveillance System (WHO-GLASS), which addresses the critical issue of antimicrobial resistance (AMR). According to the WHO, AMR represents a "global health security threat that requires concerted cross-sectional action by governments and society as a whole" (World Health Organization 2014, XIII). Additionally, the WHO describes GLASS as a "system that enables standardized global reporting of official national AMR data" (World Health Organization 2015b, 7). Recognized by the WHO as one of the top ten global threats to public health (World Health Organization 2020b), AMR highlights the urgent need for global coordination. The case study focuses on GLASS and AMR data concerning selected bacterial pathogens in the Americas that impact human health. Through this case study, the analysis explores how security and health regimes interconnect, particularly in the interplay between human and nonhuman actors.

In particular, the study analyzes publicly available information from the GLASS database to identify and examine collaboration among actors engaged in AMR. The case study suggests that security governance through OSINT promotes the emergence of a health regime to monitor infectious diseases through the following actions:

1. Diverse actors such as nation-states and institutions convene conferences and meetings and adopt collaborative regulations.
2. An international health organization facilitates collaboration on the control of infectious diseases.
3. A global threat of infectious diseases structures processes, rules, and institutions for global health governance.
4. A global technology database connects state and institution functions as a boundary object working as an inscription device that facilitates the transmission of information between actors.

Furthermore, this research examines the collaborative utilization of open-source intelligence–specifically, publicly available information from the WHO-GLASS database–to investigate collaboration among actors to counter the threats posed by infectious diseases. Through research interviews, it became evident that a more conceptual approach was necessary to effectively structure discussions on security governance in the context of data control and disease surveillance. Additionally, the inspiration for this study extended to the microbes themselves, encompassing the evolution of pathogens and the management of infectious diseases. Within the GLASS, various global actors actively participate in monitoring infectious diseases.

The initial case study centered on an in-depth examination of network state actors over time, showcasing their collaborative efforts to combat infectious disease threats transcending national boundaries. This research specifically focused on AMR surveillance of eight bacterial pathogens while also contextualizing the emergence of COVID-19 as a novel security threat and empirical evidence of interconnectedness. Although the broader research spans 2015-2021, the appearance of COVID-19 in late 2019 and its global impact in 2020 underscored the critical role of collaboration, data sharing, and security governance in addressing such crises. The pandemic offered a unique lens to evaluate the adaptability and responsiveness of security governance mechanisms amidst emerging global health threats.

The study focused on three key questions: Which actors conform to a system of rules (security governance) in response to a threat? How many WHO member-states from the southern subcontinent of the Americas contributed to the collaborative GLASS during the research timeframe? How does the security governance process, facilitated by open-source information, promote the emergence of a health regime for monitoring infectious diseases? The increased engagement of interconnected actors within our ever-changing and globalized world propels progress. Moreover, interconnectedness of actors contributes to the regulatory and security governance process, with the WHO playing a crucial role in facilitating solutions and acting as a bridge between member-states and boundary objects.

The case study illustrates the promotion of a health regime through various contributing factors. These factors include states that prioritize the issue by elevating it on the international agenda and organizing conferences to address the subject matter. Additionally, the involvement of an international health organization plays a vital role in facilitating collaboration among different actors. Furthermore, the emergence of new threats, such as infectious diseases, necessitates the establishment of systems of rules governing global health and security. Technological advancements further facilitate the exchange of information in this context. It is also important to consider additional security threats, such as cyberattacks, which may arise as a result of the initial threat. This chapter delves into the investigative nature of addressing the central research question, namely, why did security governance through an OSINT technology database of the WHO promote a health regime on the surveillance of communicable diseases in the Americas from 2015 to 2021?

As discussed in chapter 1, to answer the core research question the research analyzes the case study in conjunction with five dimensions of security governance: heterarchy, interaction, institutionalization, ideas, and a collective purpose (Webber et al. 2004; Rosenau 1992; Holsti 1992). As previously indicated in the Introduction of the book, the dependent variable is the perception of nonconventional threats in the emergence of a health regime. The independent variable is the security governance of infectious diseases. The security governance of communicable diseases influences the perception of nonconventional threats in the emergence of a health regime measured through open-source intelligence. The study looks at the control of diseases and the data during information exchange through publicly available information on the surveillance of infectious diseases. As intervening variables or an intermediary that looks to disrupt the link between the independent and dependent variables, the case study also analyzes and reviews outside factors such as the potential manipulation of human bias, algorithms, restrictions in the spread of data exchange, lack of timely information, weaknesses in the policy instrument, and countries beset by internal administrative conflicts. Thus, through the lens of security governance, the case study seeks to explain the control of diseases and data and the results of the actions of actors that tip the scales of the socioeconomic actor network.

The scope of the data collection was limited to the timeframe 2015–2021. During that timeframe, the WHO developed the GLASS for the surveillance of eight bacterial pathogens that infect human beings. In addition, the GLASS results arise from a global collaborative effort in the surveillance of AMR (World Health Organization 2017b). Thus, the surveillance of AMR supports notification of outbreaks of infectious diseases, and the GLASS network supports data sharing and member-states in their efforts to survey AMR at a global level.

Surveillance mechanisms inform "policies and infection control and prevention responses" (World Health Organization 2015b, 3). A key requirement for a successful surveillance system in response to threats to health security includes collaboration, communication, and harmonization between regional, national, and international organizations and actors. Similar to AMR, the coronavirus remains a focus of attention for health authorities, institutions, decision-makers, stakeholders, and government officials across countries. In addition, the novel infectious disease serves to place the research in context and reinforces the investigation because the novel disease is connected to the surveillance of infectious diseases. Therefore, the case study intends to inspire thought-provoking analysis and emphasize actor-network interconnectedness and the involvement of technology in the surveillance of the primary GLASS pathogens and other infectious diseases that appeared during the study, such as COVID-19, as context research.

This chapter is divided into four sections. The first section provides data analysis and results of the data collection in chapter 2. Based on the data analysis, a discussion of communicable diseases follows in section 3.2, showcasing the increase of nonconventional threats (infectious diseases) and the actors contributing to the collaborative network. The section also explains the pathogens, because the explanation allows fluidity of thought in undertaking the remaining empirical work regarding the type of threat within the health care sphere that raises security concerns. The third section furnishes the security governance metrics framework, which acts as a blueprint and baseline for the final section, which discusses the dimensions of security governance. Therefore, the utilization of data analysis, nonconventional threats, metrics framework, and features allows for a comprehensive assessment of potential risks and benefits in the collaboration and interconnectedness of actors within future security governance mechanisms.

Data Analysis: Quantitative and Qualitative Data Structures

This section presents the data analysis and results of phase 1 involving quantitative data structure, as well as those of phase 2 involving qualitative data structure. These analyses contribute to the construction of collaborative networks and facilitate the interpretation of contextual relationships among actors within the network, focusing specifically on monitoring diseases and controlling data during information sharing.

Phase 1: Quantitative Data Analysis in Tracking the Interaction of Actors to Construct a Network

Significant emergency matters affect the health of individuals surpassing the risk of infectious diseases. Collaborating with different actors is fundamental to preparedness, response, and risk reduction during crises. This research views threats to national security, such as infectious diseases, through a philosophical lens. The way people and things interconnect and collaborate in combating a threat presents some headspace for egalitarian thought. The horizon is broadened, and the actor network is traced by replacing "actors of whatever size by local and connected sites instead of ranking them into micro and macro" (Latour 2005, 179). The actors reveal the narrow collaboration space, and the network explains the trail of interconnectedness. Thus, the actors are sorted through the telescope of international studies using macro- and meso-level analysis, while also allowing ample space to explore other realms of actor inquiry and investigation. Additionally, the prismatic scope of this research is broadened with science and technology studies, followed by the utilization of ANT as a theoretical lens and network analysis as composition. This interdisciplinary approach provides the most suitable methodological framework for sorting the relevant actors and mapping the network.

Which actors enhance or detract from the network? In selecting actors in the network, contributions from ANT were incorporated, including the utilization of technologies of translation and inscription, black-boxing (erasing or normalizing), and network analysis. The actor network theory focuses on heterogeneous networks of human and nonhuman actors constructed by defending change models and building collaboration. Latour (2005) warns against discriminating between the human and the nonhuman and suggests that we should center on actors–whether human or nonhuman, skilled or unskilled–that exchange properties. Adopting a holistic view allows the contribution of human and nonhumans to flourish in network analysis. Things and objects have an agency that influences actors to do or not do certain things (Latour 2005). Thus, this research includes policy instruments such as the IHR and infectious diseases as nonhuman actors participating in the collaborative network. The introduction of contagious diseases as nonhuman actors in the network changes the thought process of production that redefines the threat to security and perceptions of collaboration.

This research also includes actors such as nation-states and organizations that collaborate in the surveillance of infectious diseases. Moreover, in Winner's felicitous terms, "technologies are not merely aids to human activity, but also powerful forces acting to reshape that activity and its meaning" (Winner 1986, 6). Thus, used as a context, technological entities such as the GLASS platform become another actor in the collaborative network. Furthermore, introducing the technology database as a node in the surveillance practice of infectious diseases transforms what participating countries do in the system. Therefore, this study focuses on all types of actors to map the network.

Moreover, this study uses the criterion of mutual relevance (Knoke and Kuklinski 1982; Laumann, Marsden, and Prensky 1982) to set boundaries in the network. The realist approach draws upon four pieces of empirical evidence: positional, decisional, repetitional, and relational (Knoke and Kuklinski 1982). During the boundary specification process, the four pieces are adopted by extracting from the data collection formal organizations with *prima facie* interests (positional), groups appearing at congressional hearings (decisional), influential groups (repetitional), and organizations named by organizational representatives during interviews (relational). However, a completely realist approach is avoided, and a more progressive mainstream liberal institutionalist approach is preferred in establishing the boundaries. Actors with no direct edge links to the interest in the substantive area but are part of the overall system are included because mutual relevance "does not always set precise and definite boundaries" (Knoke and Kuklinski 1982, 26). Limiting the network to only those linked, and excluding actors disregarding common interests, weakens the network. Thus, a complete network of actors is essential for enhancing productivity and facilitating the analytical process, contributing to the production of comprehensive results in network analysis.

Similarly, in addition to the selection of a specific sampling unit, the relational form and content (Knoke and Yang 2008, 1982) are determined based on shared interests and modes of interaction when collecting the data. On the one hand, the content was based on the surveillance of infectious diseases and the reporting of AMR. On the other hand, it was based on the fight against novel threats, such as COVID-19. The actors' drive is to combat the global threat of infectious diseases since "microbes do not respect national boundaries" (World Health Organization 2017b, 7). The type of form used in selecting and narrowing down the different actors in creating the network was based on the modes of interaction to attain a social reality. Furthermore, during the selection process, this study focused on the actors' actions, observing the actors as they conducted, and participated in, official meetings, the creation of official reports, interviews, and participation in the surveillance system of infectious diseases. These actions were monitored as they provided veridical perceptions of the security threats that were triggered.

Likewise, it is essential to be aware of the limits of a technology application that includes threats to public health and safety, exhausts valuable resources, degrades environmental quality, and causes societal stress (Winner 1986). In removing the technology database from the network, would the actors still interconnect in the surveillance of infectious diseases? The COVID-19 outbreak illustrates the interconnectedness and collaboration of actors when a threat to national security appears with or without a surveillance technology platform. Along the same lines, the pandemic has shown that other innovations have developed in the technology ecosystem, whereas in other instances, when a nontraditional security threat arises, actors are forced to use technology platforms and adhere to a new norm to sustain economic growth. Thus, the type of form was limited to actors engaged in collaboration across the corresponding setting between nation-states and institutions. This study shows that participating nation-states fed their country profiles and information into the GLASS technology platform. The participating countries, delegates, and institutions met with HHS representatives to discuss issues on AMR. Stakeholders convened to discuss national security in response to the threat of infectious diseases. Thus, the study includes participating countries, institutions, and stakeholders in the actor-network design.

Collectively, the diverse content encompassing social and economic interests is manifested through collaboration among participating countries and institutions. The collaboration establishes instrumental relationships, where actors, both human and nonhuman, connect with one another to ensure the adequacy of shared information while adhering to the IHR. As demonstrated in the analysis, the WHO relies on collaborating countries to "conduct their own national surveillance" and contribute data to the GLASS reporting platform (World Health Organization 2016b, 1). In the United States, the AMR surveillance system consists of three components: a national coordinating center, a national reference laboratory, and the AMR surveillance sites (World Health Organization 2016b, 3). This generic content or communication relationship enables the identification of interconnected actors relevant to the network. Consequently, the network includes the AMR, NRL, and NCC as actors linked to boundary objects.

Furthermore, the analysis of data in this study involves examining the intersection between an egocentric network and complete network analysis (Knoke and Kuklinski 1982). Official reports including SITREP, congressional hearing reports, and ministry of health reports serve as key sources for the analysis. The focus is on the GLASS monitoring infrastructure, extracting relevant actors interconnected in the network and linked to the boundary objects: GLASS, the IHR, and infectious diseases. Does a specific tie exist between the GLASS and all other relevant actors? Similarly, is there a link between the IHR and the actors in the network? Shifting focus from GLASS to the WHO as an institution, the study examines whether the landscape of interconnectedness promotes a change in the health regime. The intensity or strength of relations is also explored. Additionally, the study considers whether these actors would still collaborate in the fight against new and emerging threats of infectious disease if the GLASS surveillance platform were to be removed as the primary focal point. The findings highlight the WHO, the ministry of health, the PAHO, and nonhuman actors such as infectious diseases, the GLASS database, and the IHR as the main actors in the collaborative network.

However, further analysis reveals that private interest groups and NGOs, such as the Bill & Melinda Gates Foundation, academic institutions such as the Columbia University's Mailman School of Public Health, and other institutions such as the HHS and the CDC play a role in the collaboration and interconnectedness of actors. All these diverse but interconnected actors were input into the Gephi software program to create the graphs and the networks. Given the dependent variable, namely the perception of nonconventional threats in the emergence of a health regime, this study focuses primarily on infectious diseases as the main subject of global actor interconnectedness. Infectious diseases, as a nonhuman actor, represent a significant nonconventional threat to national security.

Additionally, the actor nodes representing infectious diseases were entered into Gephi, enabling the examination of a health regime as the central unit of analysis. Moreover, choosing this boundary object as the center of gravity in creating interconnectedness encompassed the GLASS human-priority pathogens and the novel COVID-19. Furthermore, a collective purpose or a common interest, such as combating AMR, triggers security governance. "AMR is a global health security threat that requires concerted cross-sectional action by governments and society as a whole" (World Health Organization 2014, XIII). Additionally, the security governance of data sharing in the surveillance of infectious diseases requires involvement from diverse actors, including those at the top, bottom, local, and national levels, public and private sectors, and various industries (Clark-Ginsberg 2020; Berthod et al. 2016). Thus, once a national security threat emerges, actor reaction, linkage, and deflection commence, triggering security governance.

Moreover, during the scope of the investigation, various meetings were held by the HHS, including those of its council members and federal representatives, to discuss the global problem of antimicrobial and antibiotic resistance. For instance, in 2016, Argentina, Brazil, Ecuador, and the United States participated in a high-level meeting on AMR convened by the President of the General Assembly of the United Nations. The participating countries enrolled in the GLASS database from global South included Argentina and Brazil. In addition, in 2016, global leaders, heads of state, and heads of delegations met at the United Nations General Assembly to commit to the fight against AMR. One of the panelists was the Minister of Health of Argentina. In addition, NGOs, civil society organizations, and academic institutions participated in the high-level meeting on AMR.

Indistinguishably, just as global leaders came together to combat the threat of AMR, the COVID-19 pandemic brought astronomical political, economic, and cultural repercussions. In March 2020, leaders of the seven wealthier nations–Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States–held the G7 summit via teleconference to discuss the impact and challenges of COVID-19 (The White House 2020). Likewise, in March 2020, the G20 leaders held an emergency videoconference to coordinate efforts in response to the COVID-19 pandemic (G20 Saudi Arabia 2020). Furthermore, in September 2020, the PACCARB, supported by the HHS, held a virtual meeting to discuss the impact of COVID-19 and its effect on AMR (U.S. Department of Health & Human Services 2020a). Finally, in November, the 2020 G20 Riyadh Summit was held virtually and included a discussion on handling global threats such as the COVID-19 pandemic (G20 Riyadh Summit 2020).

Global pandemics, cybercrime, and emerging technologies bring diverse actors together to combat nontraditional threats, which have come to the forefront of the international agenda as issues of concern for civil societies and nation-states that serve them. For example, in March 2020, elite hackers attempted to break into the WHO (Satter, Stubbs, and Bing 2020). Not only did the world have to confront a pandemic attack, but countries, too, had to battle hacking attempts. Thus, the quantitative analysis commenced by establishing connections between the primary actor (infectious diseases) and other actors who shared a common interest in virus surveillance, disease control, and outbreak containment. This collaboration and interconnectedness among actors were primarily driven by the potential national security threat posed by infectious diseases, prompting swift action.

Choosing relevant actors to create the network entails opening the political and social network to understand the complex relationships that develop in promoting a health regime. Limiting the network to specific actors, such as choosing only executive, legislative, and private groups, does not explain the changes in the interconnection of actors and the reasoning behind actor participation when there is a common interest. Thus, the study highlights the interplay between diverse interests and collaboration, including activities such as meetings focused on AMR and infectious diseases, allocation of funds, academic research initiatives, participation in forums addressing national security concerns, and sessions involving various countries and institutions.

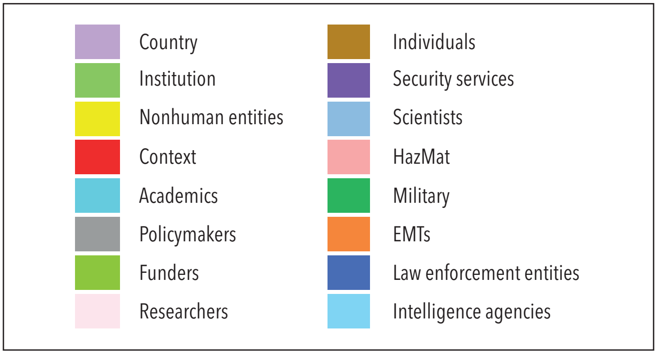
Moreover, intermediary groups, including private interest groups and academic universities with shared interests, contribute to the expansion and diversification of the network. To construct the network, the data were encoded by classifying the actors into 16 categories: academic institutions, contextual groups, nation-states (countries), funding partners, hazardous materials response teams (HazMat), individuals, general-type institutions, intelligence agencies, law enforcement entities, emergency medical teams (EMTs), the military, nonhuman entities, policymakers, researchers, scientists, and security organizations. This specific categorization enabled the construction of the network.

Mapping the Network

This section provides details of statistical analysis and scientific information. To create and map the networks, the premise of this study commences with two goals: (1) to develop maps that illustrate the relational links that actors have to infectious diseases and (2) to create a map that shows the interconnection of actors with each other based on a nontraditional security threat such as infectious diseases. Four distinct network paths were mapped as a result of the process to design a structure for quantitative data. Figure 3.1 lists the 16 categories mentioned above, each represented by a distinct color.

The sixteen categories and the color representing each category (as shown in figure 3.1) are as follows: country (pastel purple), institution (asparagus green), nonhuman entities (yellow), context (red), academics (pale teal), policymakers (gray), funders (lime green), researchers (pastel pink), individuals (pale brown), security services (vibrant purple), scientists (sky blue), HazMat (salmon pink), military (clover green), EMTs (orange), law enforcement entities (blue), and intelligence agencies (light blue).

Figure 3.1. Categories of actors and the colors representing each category



Determining the appropriate methods and findings means concentrating first on one path, sorting through the mass of issues, such as those involving public health, and taking each separately to make sound judgments (Winner 1986). To create the visual representations, four types of nodes and edge paths were created, focusing on the intersection of public health and security in promoting a health regime. The nodes in the graphs represent objects, whereas the edges represent the relationships between them. Here, the nodes represent the different actors in the network. The edges, perceived as object A to object B, represent the interconnection of actors through the review, observation, and analysis of official meetings, events, or documents that exist from actor A to actor B, and so forth. This study's dataset comprises the 16 categories. Furthermore, these actors provide examples of theoretical representation to strengthen global health, the surveillance of AMR, and collaboration through data sharing to combat infectious diseases such as COVID-19 and those caused by the GLASS pathogens.

The first network, CNPA, includes the GLASS database and the GLASS pathogens as nonhuman actors (nodes) and research context that helps shape the research. In this design, the nodes contain the actors connected only to the GLASS platform. The network excludes the nonhuman actor COVID-19, as the threat occurred during the latter part of the investigatory process. In this design, rather than separately listing the names of each of the selected GLASS pathogens, this study coded the eight bacteria nodes under one label, namely pathogen.

The second network, CNPB, includes nodes where the focus is only on the GLASS technology database. What happens to the network after removing the threat (infectious diseases) and the technology database created as the glue that links all actors? How is a database capable enough to connect the actors or to persuade them to collaborate without disease as a trigger? This research removed the nonhuman actor, GLASS pathogens, and only included the GLASS technology database as the main actor. Therefore, technology remained the main focal point of design and showed how technological advancements connect all relevant actors in the network.

In the third network, CNPC, the nodes are exclusively associated with the GLASS pathogens as a known threat. In this design, a different approach was taken. The GLASS database was not considered an actor; instead, the GLASS pathogens served as the focal point. Relevant actors were then linked to this focal node in the network. The study further separated the eight bacterial pathogens that infect human beings and connected them to their respective target GLASS countries. This scenario illustrates how the threat is the common nucleus that fuses all relevant actors and the potential irrelevance of a technological actor or technological advancements in the collaborative sphere. Therefore, this design strives to illustrate how a public health crisis triggers actor collaboration.

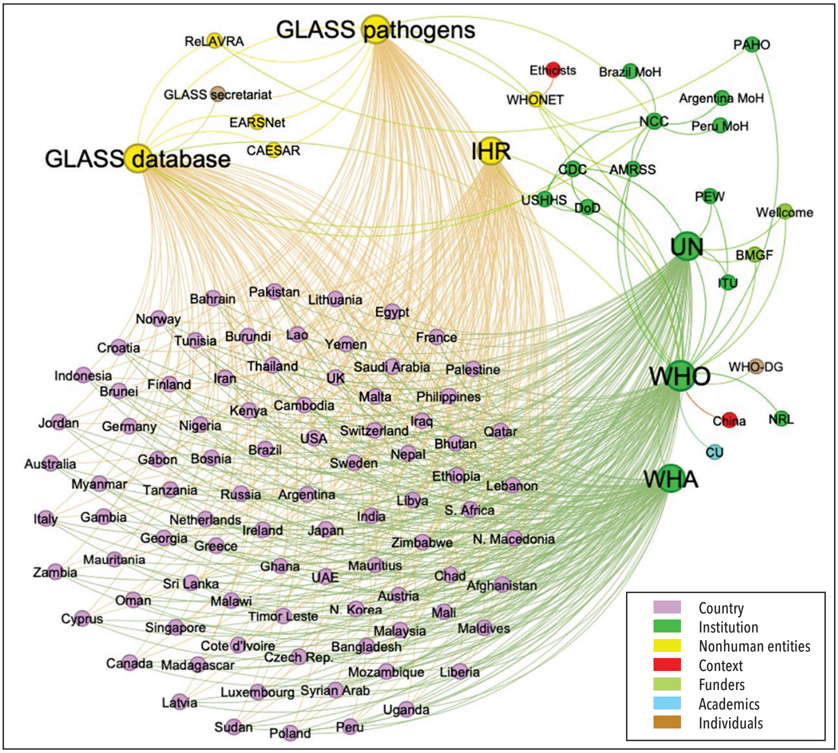
In the fourth network, CNPD, the infectious diseases node was chosen as the center of gravity or the focal point that connects all relevant actors to the boundary object. In this design, the study includes the COVID-19 virus, an unknown novel threat, to illustrate and reinforce the diverse but interconnected network of actors with a common interest: to eradicate a threat in the interest of national security. Thus, this path distinguishes the nodes as the GLASS database, GLASS pathogens, and the coronavirus. Furthermore, this design further breaks down the category into two different nodes, GLASS pathogens and COVID-19, by giving the nodes separate code names, which allows the expansion of analysis and comparison between the interconnection of actors from the perspective of the original pathogens versus the novel coronavirus. Thus, as with CNPC, the threats trigger the actors to collaborate and interconnect.

Displays: Network Visualization and Analysis

The sociogram visualizations (Figures 3.2, 3.5, 3.6, and 3.7) were prepared by the author using the Gephi software and the Force Atlas algorithm model. Data for these visualizations was sourced from the GLASS and ReLAVRA database. This force-directed layout brings connected nodes together inside the network and moves unconnected nodes outside the network. Network analysis "offers a powerful brush for painting a systematic picture of global structures and their components" (Knoke and Kuklinski 1982, 10) and accesses systems comprising node points that serve a function and edges, which are connections that link to the nodes (Clark-Ginsberg, Abolhassani, and Rahmati 2018; Kalyagin, Pardalos, and Rassias 2014). Besides, network analysis helps in discovering complex data patterns such as those that show how interdependencies shape risks (Clark-Ginsberg, Abolhassani, and Rahmati 2018); in analyzing policymaking (Marsh and Smith 2000); in understanding social networks (Knoke and Yang 2008); and in studying statistical procedures in the economic market (Kalyagin, Pardalos, and Rassias 2014). Moreover, statistical analysis estimates the probability of various scenarios or events being correlated (Winner 1986). Therefore, a myriad of different disciplines use network analysis.

The first network, CNPA, includes nodes with two main focal points: technology database and infectious diseases. A graph was generated using Gephi to visualize the connections among actors in the network. The actor-network design consists of 117 nodes and 571 edges. Figure 3.2 shows the network, highlighting connections between actors when focusing on the GLASS surveillance platform and selected pathogens. This initial network path serves as a primer, introducing new colors and providing the contextual framework for the subsequent three path designs, all three being influenced by this overarching network structure.

Figure 3.2. Sociogram of collaborative network Path A (GLASS and GLASS-selected pathogens)



Source: Prepared using Gephi with the Force Atlas algorithm model.

The results from the CNPA network show an undirected network interpretation parameter, graph density of 0.084, and an average degree of 9.761. Another centrality measure, PageRank, calculates which "important node receives connections from many other important nodes" (Lambiotte and Schaub 2021, 19). The results show parameters with a probability equal to 0.85 and an epsilon of 0.001, with most nodes clustered at the lowest count from 0 to 5 and one node reaching a count of 90. Furthermore, the results show that the ego's network CNPA consists of two weakly connected components. The results further illustrate an average clustering coefficient of 0.416 as the mean value of individual coefficients with a parameter of 100 iterations. This study employs two centrality measures, eigenvector centrality and betweenness centrality, as analytic techniques to understand the network results. The eigenvector centrality is based on a circular argument, where important nodes are, by definition, nodes adjacent to many important nodes (Clark-Ginsberg 2020; Borgatti, Everett, and Johnson 2013; Knoke and Kuklinski 1982). For example, figure 3.3 provides the formula of the eigenvector centrality which shows that *e* represents the score of the eigenvector centrality and lambda (λ) represents the eigenvalue, a proportionality constant (Borgatti, Everett, and Johnson 2013).

Moreover, the eigenvector illustrates the importance of nodes within a network. In this study, the eigenvector centrality distribution shows nodes with a high score of 1, implying greater influence on the network. The betweenness centrality measures how frequently a node appears on the shortest path between two network nodes (Clark-Ginsberg 2020; Borgatti, Everett, and Johnson 2013; Knoke and Kuklinski 1982). Figure 3.4 provides the formula of the betweenness centrality of node *j*, in which $g(ijk)$ represents the number of geodesic distance (shortest path) that connects *i* and *k* through *j*, and $g(ik)$ represents the number of geodesic paths that connect *i* and *k* (Borgatti, Everett, and Johnson 2013).

In this research, the betweenness centrality distribution results in a diameter of 5, a radius of 0, and an average path length of 2.022 rounded off to three decimal places. It is important to review the mutually reinforcing

Figure 3.3. Formula for Eigenvector centrality

$$e_i = \lambda \sum_j x_{ij} e_j$$

Source: Borgatti, Everett, and Johnson 2013.

Figure 3.4. Formula for the betweenness centrality

$$b_j = \sum_{i<k} \frac{g_{ijk}}{g_{ik}}$$

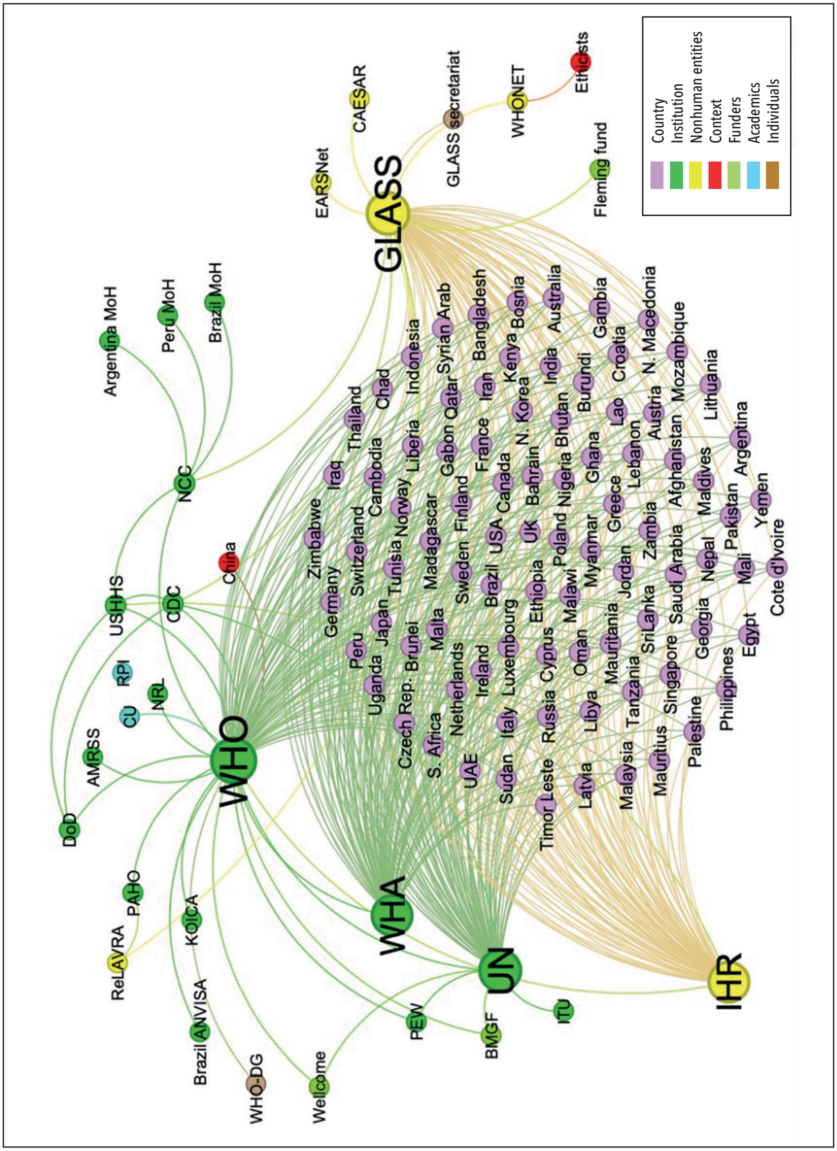
Source: Borgatti, Everett, and Johnson 2013.

relationships between hubs (Kleinberg 1999), which looks at good relationships. Graphs with mutual relationships illustrate a strongly connected relationship (Borgatti, Everett, and Johnson 2013; Kleinberg 1999). The hyperlink-induced topic search (HITS) measures the quality of the node's link (Borgatti, Everett, and Johnson 2013; Kleinberg 1999): in the present case, the HITS metrics are E = 1.0E – 4 parameter, and a hubs' distribution score of 0.5 ranging between 5 counts at the lowest spectrum to 90 counts at the highest spectrum.

Lastly, to assess the network's vulnerability, the size distribution of the modularity or community detection was examined (Borgatti, Everett, and Johnson 2013; Blondel et al. 2008). As another measure, modularity compares the edge density within a community to the edge density between communities and also the number of internal links to an expected number distributed at random (Borgatti, Everett, and Johnson 2013) and thus helps to analyze network communities by identifying the nodes densely connected to each other (Blondel et al. 2008). A community emerges as a group of nodes more densely connected to each other than to the rest of the network. Thus, modularity gives a general idea of the structure of the network. In the present study, the modularity in five communities was 0.050. Since the results have a low modality, there are fewer vulnerabilities by having these actors interconnected in the network. Thus, the design shows a positive interconnection when the GLASS database and GLASS pathogens are the focal points. However, it is important to consider whether the results were influenced or skewed by the information added as inputs, adjustments to new actors, and changes in the focal point during data collection and analysis. Subsequently, the context from CNPA was utilized to develop two additional designs, CNPB and CNPC.

The second network, CNPB, includes nodes with only the GLASS database. This study removes the GLASS pathogens from the CNPB network. A Gephi graph analysis was conducted to examine the actors connected to the network when infectious diseases were removed from the scenario. This actor network contains 119 nodes and 477 edges. Figure 3.5 shows the different connections of actors in the network when the focus is away from infectious diseases and toward advancements in technology. In this case, the

Figure 3.5. Sociogram of collaborative network Path B (GLASS)



Source: Prepared using Gephi with the Force Atlas algorithm model.

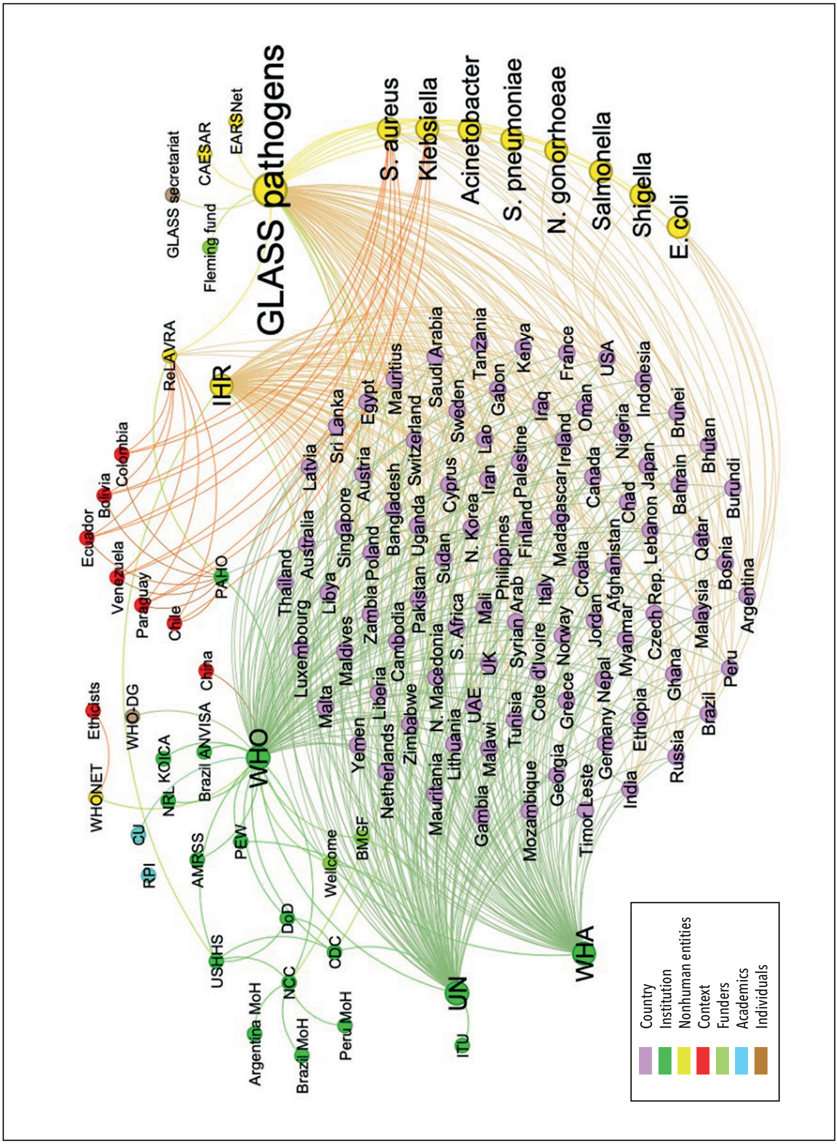
main actor is the GLASS technology database. Now the process of adding colors to the canvas and analyzing how the actor network becomes a painting can begin. Does the network begin to show further interconnectedness, or do the actors remain the same with lower degrees of centrality?

The results from the CNPB network show an undirected network interpretation parameter and graph density of 0.034 with an average degree of 4.008. The results show parameters with a probability equal to 0.85 and an epsilon of 0.001, with most nodes clustered approximately from 0 to 9 counts and one node reaching a count of 90. Furthermore, the results show that the ego's network consists of two weakly connected components and an eigenvector distribution with a high score of 1. The results also illustrate an average clustering coefficient of 0.393 as the mean value of individual coefficients with a parameter of 100 iterations. The betweenness centrality distribution results in a diameter of 5, a zero radius, and an average path length of 2.02, rounded off to two decimal places. The mutually reinforcing relationship (Kleinberg 1999) of the nodes with the largest connections to many authorities results in a hubs' distribution of a little over 0.5 scores with a range from 0 to more than 80 counts. The HITS metric report shows no counts listed between the 10-80 range under a parameter of $E = 1.0E - 4$.

To assess network vulnerability, the modularity report was analyzed, revealing a modularity of 0.054 distributed across five communities. However, it is worth exploring whether the results would differ if the interconnection of actors is examined from a different perspective, specifically through the lens of the GLASS pathogens. Consequently, a new network, CNPC, was created, this time excluding the GLASS database. In this scenario, the focal point shifts to the GLASS pathogens themselves. The nodes in this network include all eight bacterial pathogens affecting human beings, allowing for a more detailed analysis of how the actual threat, acting as a common nucleus, connects to different actors within the network.

In the third network, CNPC, only the nodes representing the GLASS pathogens were included. Figure 3.6 shows the outcome of removing the GLASS database from the network to focus solely on the actors. When the technology database was removed, a Gephi graph analysis was conducted to examine the actors connected to the network. This actor network

Figure 3.6. Sociogram of collaborative network Path C (GLASS pathogens)



Source: Prepared using Gephi with the Force Atlas algorithm model.

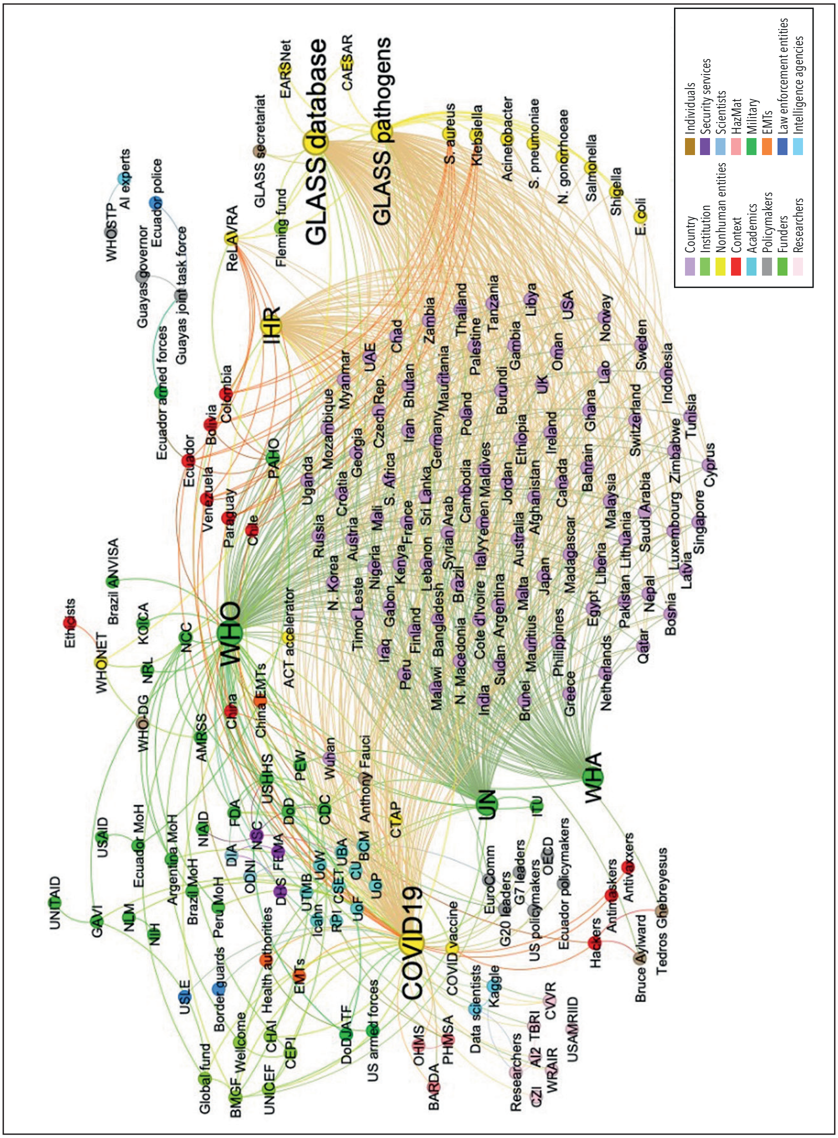
consists of 133 nodes and 537 edges. The CNPC network demonstrates how different actors connect within the network, with the GLASS pathogens serving as the point of convergence.

The results from the CNPC network show an undirected network interpretation parameter and a graph density of 0.061 with an average degree of 8.075. The results show parameters with a probability equal to 0.85 and an epsilon of 0.001, with most nodes clustered approximately from 0 to 6 counts and 1 node reaching 80 counts. Moreover, the results show that the ego's network consists of two weakly connected components. Furthermore, the results illustrate an average clustering coefficient of 0.382 and an eigenvector centrality with a high score of 1. The betweenness centrality distribution results in a diameter of 4, a zero radius, and an average path length of 2.10, rounded off to two decimal places. The mutually reinforcing relationship hubs (Kleinberg 1999) result in clusters with 0 and 0.5 scores in two distribution areas.

A modularity report was analyzed to assess the network's vulnerability, revealing a modularity of 0.175 distributed across five communities. How will the actor network change in the subsequent design stage when the network introduces a new actor that mirrors one of the original primary actors? During the investigation, a novel infectious disease occurred, COVID-19. Like the GLASS pathogens, which interconnect actors within a complex world, the global occurrence of COVID-19 served as a reinforcement mechanism for the research study. Since the coronavirus infectious disease influenced diverse actors in the international system, the following CNPD design includes COVID-19 as a security threat.

The fourth network, CNPD, includes nodes interconnected with the GLASS system, GLASS pathogens, and the novel COVID-19. The premise of this design path showcases how threats such as infectious diseases significantly influence the interconnection and collaboration of actors in the network-known diseases (pathogens showing AMR) versus unknown diseases (COVID-19). Does the network landscape change with the introduction of a novel infectious disease? Do the actors continue to collaborate on AMR pathogenic issues or refocus the surveillance on the new threat? The CNPD network in figure 3.7 includes all primary nodes of network

Figure 3.7. Sociogram of collaborative network Path D (GLASS, GLASS-selected pathogens, and COVID-19)



Source: Prepared using Gephi with the Force Atlas algorithm model.

actors to identify the actors that interconnect. This actor network contains 201 nodes and 864 edges. The point of convergence consists of an infectious disease beyond the scope of GLASS pathogens and the GLASS database in the surveillance of an outbreak.

The results from the CNPD network show an undirected network interpretation parameter and graph density of 0.043 with an average degree of 8.597. The results show parameters with a probability equal to 0.85 and an epsilon of 0.001, with most nodes clustered approximately from 0 to 14 counts and one node reaching 80 counts. Moreover, the results show that the ego's network consists of five weakly connected components. The results also illustrate an average clustering coefficient of 0.458 and an eigenvector centrality measure with a high score of 1. The betweenness centrality distribution results in a diameter of 5, a zero radius, and an average path length of 2.19, rounded off to two decimal places. The mutually reinforcing relationship (Kleinberg 1999) results in a hubs' distribution where clusters appear between a score of 0 and 0.5. Lastly, a modularity report was analyzed to assess the network's vulnerability, revealing a modularity of 0.256 distributed across seven communities.

About Scientific Mumbo-Jumbo: Network Path Analysis

In the preceding paragraphs, a number of scientific analyses were presented along with the corresponding visuals. However, it is important to consider the implications of these findings and how they can be understood and appreciated by a broader audience. By examining the visualization maps, one can gain insight into the various participants within the network, the interconnected subgroups, and the individuals who hold a significant influence. Such information has practical applications in understanding and relating to real-world scenarios. In context, the maps illustrate how certain actors, such as infectious diseases and technology, are embedded in interconnection challenges. The results show that the greater the security threat, the higher the interconnection of actors. As AMR or COVID-19 challenges increase, other issues arise, problems are heightened, and more actors introduce themselves into the network.

While mapping the networks, 16 actor-theme categories were used for encoding the data. The network consists of nodes (entities that remain the same over time) and edges (relations, interconnections, or temporary connections). In this study, the CNPA path comprises 117 nodes and 571 edges; the CNPB path, 119 nodes and 477 edges; the CNPC path, 133 nodes and 537 edges; and the CNPD path, 201 nodes and 864 edges. In comparing each direction, the number of nodes increased as each network grew in connections. The transition between each network from CNPA to CNPD was nonlinear. This study treated each path independently from the other depending on the focal point. However, this research reveals that the more nodes are input into the software program, the higher the transgression between edge links and increases in the number of nodes. Thus, this study shows that the paths differed depending on the focal point. For instance, the CNPA contains 571 edges with the GLASS database and pathogens as focal points whereas during the creation of the CNPB, the edges decrease with the GLASS database as a primary focal point. Similarly, the CNPD contains 864 edges when the graph network introduces the COVID-19 actor node into the system. Thus, the graphs are independent of each other.

Moreover, analysis of the CNPB with the GLASS database shows that the relational edges decrease because the actors in the network, such as the participating countries, were directly interacting with the GLASS platform but not with each other. Thus, actors outside the database sphere were not counted in the network, reducing the number of edge links. This shows a global reduction in interconnections because of the link between those associated with the platform. The CNPB's structural gap between the nodes and edges compared to that in the other paths creates an awareness of the closeness of the inner circle surrounding the GLASS platform of actors and the lack of global interconnectedness to a nonhuman actor such as a technological database. Disconnection from the platform encourages a linkage between actors.

By contrast, when the focal point changes to a global threat such as infectious diseases, for instance, the surveillance of AMR of the eight bacterial pathogens that infect humans, as illustrated by the CNPC network, an increased constellation of actor interconnection occurs. The connectivity basis in the CNPD network is expanded by the inclusion of an additional node representing the infectious disease COVID-19. This addition enhances the network's comprehensiveness and facilitates a deeper understanding of the interconnections and dynamics of the entities within the network, taking into account the influence of COVID-19. The results illustrate that the network expands. The influence of the connectivity basis of interconnectedness and collaboration between the nodes is evident in all four paths. These paths also reveal the most influential actors within the network. Furthermore, the existence of commonality serves as an additional basis for connectivity. By proposing such an alternative basis, a different perspective can be adopted to analyze and influence the network. However, in this study, the focus is on advocating for collaboration and interconnectedness among the actors to promote a health regime. Table 3.1 provides a summary of the measurements and results of the four network paths, including the following details.

The network-connected components illustrate the most shared ideology. In this case, collaboration in the surveillance or combating infectious diseases is the most shared ideology. More specifically, all four networks

Table 3.1. Selected parameter values for four collaborative networks

Network	Nodes	Edges	Density	Connected Component (union find)	Clustering Coefficient	Centrality Measure			Modularity Comm. Detection
						Aver. Degree	Max. Degree	Min. Degree	
A	117	571	0.084	2	0.416	9.761	105 (WHO)	0 (RPI)	0.050 five communities
B	119	477	0.068	2	0.393	8.017	106 (WHO)	0 (RPI)	0.054 five communities
C	133	537	0.061	2	0.382	8.075	107 (WHO)	0 (RPI)	0.175 five communities
D	201	864	0.043	5	0.458	8.597	151 (COVID-19)	0 (RPI[a], USAMRID)[b]	0.256 seven communities

Source: Prepared using the statistical analysis derived from network map results in Gephi.
[a]Rensselaer Polytechnic Institute.
[b]United States Army Medical Research Institute of Infectious Diseases.

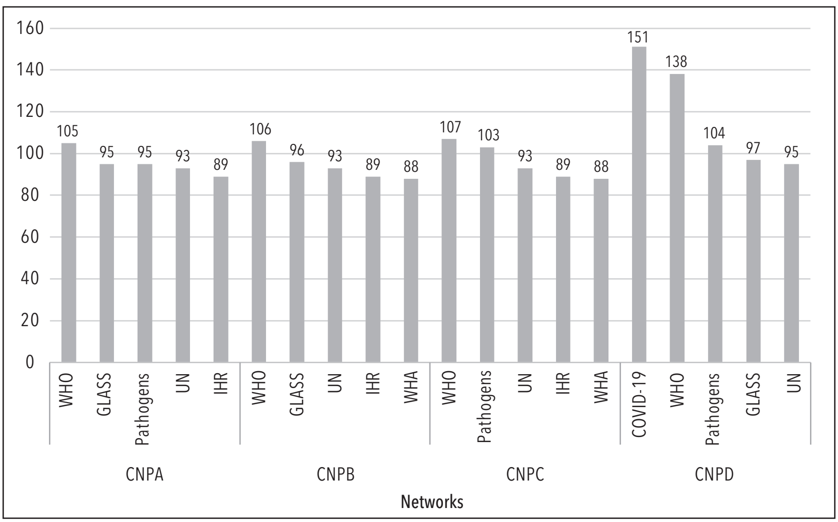
share a common ideology and the desire to collaborate in combating infectious diseases and data sharing. Therefore, CNPA shows two weakly connected components in the network; CNPB and CNPC show two connected components each; and CNPD shows five connected components. Overall, all four network paths have low union finds, which illustrates their strong connection to become interconnected when the shared ideology is based on the information from surveillance for AMR, combating the COVID-19 coronavirus, or promoting global health.

Furthermore, the clustering coefficient shows the nodes that are most densely connected in the network. The coefficient measure compares the number of connections to other nodes with the potential number of links to different nodes in the group. Collectively, all the four networks reveal that the most densely connected subgroup in the network is that of the countries participating in the GLASS database. In addition, the four networks show how institutions also form different clusters interconnected to the WHO in addressing national security threats such as infectious diseases. Similarly, under the CNPA network, where the focus lies on the GLASS database and pathogens, the mean value of the clustering coefficient is 0.416; CNPB has an average clustering coefficient of 0.393; CNPC, whose primary focal point is the GLASS pathogens, has a clustering coefficient of 0.382; and CNPD has an average clustering coefficient of 0.458. By comparison, the low value of the coefficients in each path indicates that all other actors in the network reference the nodes with the highest weight. For example, CNPC's main focal point is the GLASS pathogens and has the lowest clustering coefficient (0.382) compared to the rest of the paths. This study reveals that GLASS pathogens have a low clustering coefficient because of the link with the participating countries who collaborate by inputting AMR surveillance information on the GLASS platform.

The degree of a node represents the number of connections the node has to other nodes in the network. The higher the node degree, the more connected the nodes are to each other. Figure 3.8 shows the average degree for each network of the top five nodes. The top five actors in the CNPA network are WHO, GLASS database, GLASS pathogens, UN, and the IHR; the top five in the CNPB network are WHO, GLASS database, UN, IHR, and WHA; in the CNPC network, WHO, GLASS pathogens, UN, IHR, and WHA; and in the CNPD network, COVID-19, WHO, GLASS pathogens, GLASS database, and the UN. The WHO, an institution, plays a major role in the collaborative network as the results illustrate its placement with a high degree compared to other nodes. Overall, these top five actors have the most significant connections to the rest of the nodes in the network. Therefore, these actors have a heightened influence on the collaborative network.

In addition, link density gives the number of all ties divided by the number of all possible ties in the network and ranges between 0 (totally disconnected) and 1.00 (totally connected) (Knoke and Kuklinski 1982). The higher the density of links within a network, the greater the probability of collaboration. The density of each network was as follows: CNPA, 0.084; CNPB, 0.068; CNPC, 0.061; and CNPD, 0.043. As can be seen, the density of the CNPA network is considerably higher than that of the CNPD network. Likewise, although directed network analysis predominantly uses PageRank measures, the PageRank scores also extend to undirected graphs

Figure 3.8. Top five node degrees and their distribution, by network (based on results from Gephi)



(Perra and Fortunato 2008; Abbassi and Mirrokni 2007) to "enlighten deep and robust network properties of the graph" (Iván and Grolmusz 2011, 405). PageRank underscores the importance of a node in connection to other vital nodes, such as the most clicks on a link when surfing the web. The results of the study, shown in figure 3.9, reveal that the WHO has the highest PageRank in three of the four networks. The WHO came in as the second most important node in the fourth network. This means that many actors point to the WHO as an institutional actor. Another way to understand the importance of actors in the network is to view the analysis on the flip side. If an actor has fewer connections in the network, the quality of the collaborative contribution is low. Therefore, figure 3.9 shows the top five actors with the most PageRank importance in all four networks.

Because eigenvector centrality measures a node's influence in the network, figure 3.10 shows that the WHO has the greatest influence on all four networks with the highest score of 1. Therefore, as an institution, the WHO has a wide-reaching influence in all four networks.

Figure 3.9. Top five PageRank nodes and their distribution, by network (based on results from Gephi)

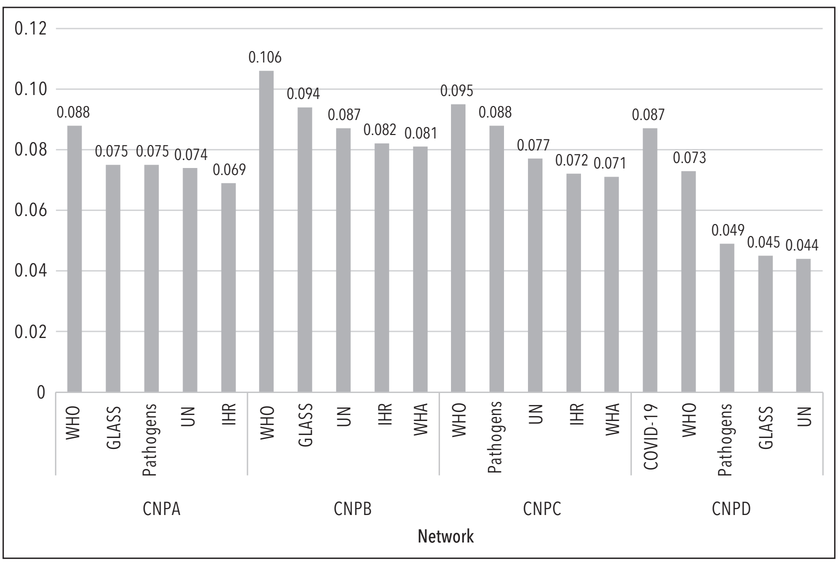
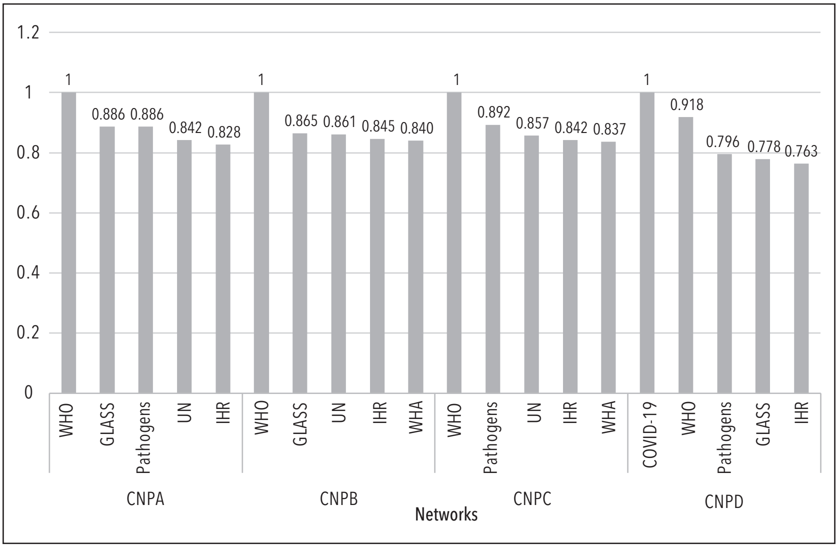


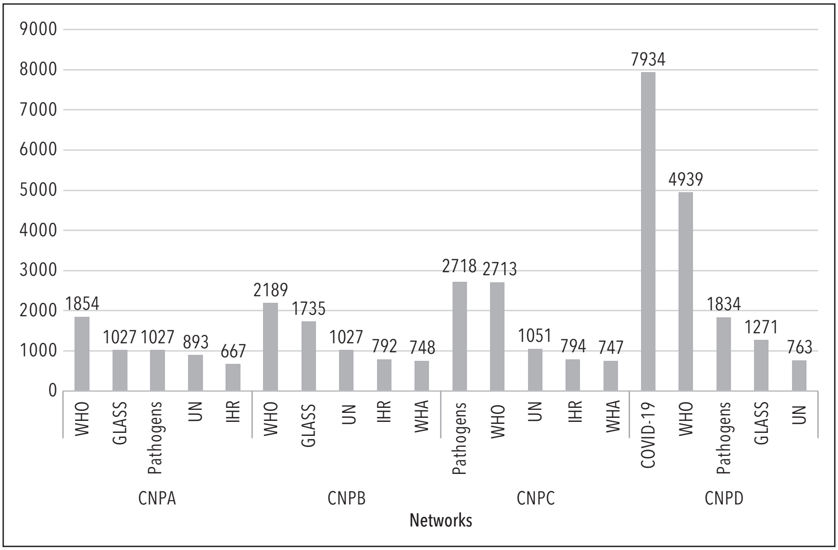
Figure 3.10. Top five Eigenvector centrality nodes and their distribution, by network (based on results from Gephi)



Moreover, of the 16 actor categories, the category 'institutions' had the most degree, with the category 'nonhuman' ranked second. Upon further analysis, the nodes most mentioned in all four paths were the WHO (institution) and infectious diseases because these nodes shared the most significant number of connections in each network. Furthermore, the networks illustrate that human and nonhuman actors play a pivotal role in network interconnectedness and collaboration with other less connected nodes.

Another critical measure of the node's influence in the network is revealed through a betweenness centrality analysis (figure 3.11). Whereas the degree looks at the number of connections between nodes, the betweenness centrality chooses nodes randomly but views how often the nodes appear in the shortest path between two randomly chosen nodes. Moreover, the betweenness centrality looks at how a node connects to the entire network (Clark-Ginsberg 2017). The statistical analysis of CNPA showed that the following nodes had the highest betweenness centrality: WHO, GLASS database, GLASS pathogens, UN, and the IHR. For CNPB, the actors with

Figure 3.11. Top five betweenness centrality nodes and their distribution, by network (based on results from Gephi)



the highest betweenness centrality were the WHO, GLASS pathogens, UN, IHR, and the WHA; for CNPC, they were GLASS pathogens, WHO, UN, IHR, and the WHA; and for CNPD, they were COVID-19, WHO, GLASS pathogens, GLASS database, and the UN. This makes sense because, for example, the participating member-states funnel their information on AMR surveillance into the GLASS rather than connect with one another. In addition, the WHO-GLASS department maintains contact with the participating member-states. Therefore, the results show that high-betweenness actors bridge those parts of a network that need to be better connected.

Comparing all four paths shows that the WHO and infectious diseases lead as primary actors, with a high degree and high betweenness centrality. The WHO, GLASS pathogens, and COVID-19 are well connected within the cluster of the whole network. More specifically, infectious diseases such as those caused by the GLASS pathogens or COVID-19 exhibit a high level of centrality, which indicates objects that play a significant role in the overall issue. This centrality is indicative of these diseases being both a contributing factor and a result within the network. The nodes collectively highlight communicable diseases as a central challenge to global health and national security, contributing significantly to economic distress and recession. Thus, addressing the threat of infectious diseases becomes crucial for both national security and civil society interests, creating a reciprocal relationship.

Moreover, the research indicates that the WHO, GLASS pathogens, and COVID-19 actors have a strong local influence on the network and a global influence over the whole network. In addition, one node actor had a high betweenness centrality and low degree. In the CNPA, the NCC had a high betweenness centrality of 501 and a low degree of 9. This is not surprising since the NCC "establishes and oversees the national surveillance program, gathers national AMR data and communicates with GLASS" through a national focal point (World Health Organization 2017b, 9). Thus, although the NCC has fewer connections, the node's connections influence the entire network as the node is a central figure within the network.

In addition, modularity, or community detection (Blondel et al. 2008), helps identify densely connected nodes. The modularity of each of the paths makes it possible to analyze communities within the network. For comparison, the 117 nodes of network CNPA show a modularity of 0.050 partitioned into five communities, the corresponding figures being 119 nodes and a modularity of 0.054 in five communities for CNPB, 133 nodes and a modularity of 0.175 in five communities for CNPC, and 201 nodes and a modularity of 0.256 in seven communities for CNPD. The study shows that the member-states participating in the GLASS do not have a significant deviation in the node and have the same size and dense connection compared to the entire network. Furthermore, the four networks reveal that the common communities comprise three categories: nonhuman (GLASS database and pathogens), institution, and country. Thus, the study shows that all four paths have a small modularity measure (< 0.3), and the networks in different communities have strong segregation.

Furthermore, for Knoke and Kuklinkski (1982), network analysis considers "both the relations that occur and those that do not exist among the actors" (Knoke and Kuklinski 1982, 12). The networks bring out the dissimilarities between the actors as measured in the relational patterns with other actors (Knoke and Kuklinski 1982). For example, the results show that, out of the four networks, the actors that have a different pattern of ties with other actors in the network are, for instance, China, ethicists, cyber threat actors, anti-maskers, and anti-vaxxers (those who believe that vaccines are unsafe and violate their human rights). Created as a context in the network, these actors are different from each other and the network space. Although these nodes disrupt the network, they do not necessarily hinder it. Instead, these actors illustrate the importance of network analysis, spurring innovation and creating interesting interconnections and collaboration with other actors in the network. The network, including the context actors that create gaps in the network, collectively reinforces aspects of collaboration. Thus, these disruptions in the network allow room for improving actor collaboration and global interconnectedness toward the path of global health and security.

In conclusion, the statistical analysis illustrates the importance of identifying the most valuable parts of the network. In mapping the four distinct networks, the focus was on extracting information about the most influential actors, examining clusters, and analyzing network properties. This analysis delved into the value of collaboration and interconnectedness within the networks-knowledge valuable in improving a network's connectivity by seeing how different actors are interconnected. The visualization offers valuable clues on the structure of the collaborative network. Mapping the diverse networks results leads to the understanding that actors make crucial choices in limiting the promotion of a health regime by not adhering to governance or a system of rules. Technical capacities expand, and communications increase. They force actors to access massive amounts of information. Some actors choose not to share data on publicly available platforms for the surveillance of infectious diseases, while others opt for limited participation by providing only partial details in the surveillance platform.

In contrast, other actors raise concerns about privacy and security measures even when combating a threat to the global common good. The complex interdependence of actors changes the process of network creation. Thus, this study shows the importance of network analysis in viewing how certain actors disrupt the network and its value in helping to understand the rhetoric of interconnection. An in-network disruption removes the node actors from the network to create more power, stability, and balance. However, removing a node either strengthens or weakens an edge connection. By contrast, another recommendation is to include the actors while considering a skewed network and its influence on other actors in the network. The access to information derived from network analysis contributes to knowledge in diverse fields. Tracking the interaction of actors and obtaining statistical data provide direct and concrete answers in an otherwise confusing and complex system of interdependence. Technology, innovation, social structures, and actor collaborations contribute to international relations, global experiences, the international and local economy, and progressive accountability–all these efficiencies derived from networks.

In conclusion, although the IHR, GLASS, and the WHO are relevant actors that link to other actors in the network, this study chose a more prevalent boundary object–infectious diseases–to act as an anchor or bridge. The boundary object encompasses both COVID-19 and the eight GLASS bacterial pathogens that infect human beings. The results of this study reveal that actors immediately collaborate in promoting a health regime when the level of threat to security goes up. Although in context certain actors appear to disrupt the network, appearing outside of the collaborative network, such as by blanketing information or striving for a hegemonic role in the international system, the actions stem from a common nucleus-triggering of a nontraditional threat such as infectious diseases. Nonetheless, the research shows that it is in the best interest of all countries for the actors to work together and interconnect in the fight against global infectious diseases because such diseases go beyond national borders.

The technological innovation ecosystem begins to function at a macro level, and actors such as collaboration agencies influence the network system. At the macro level (large systems), the collaborative network comprises actors with similar common interests and a background of known or unknown boundary objects. At the meso level, actors in the collaborative network prefer to interconnect with others with a similar interest in a specific known object (AMR). Network analysis bridges the gap between macro- and meso-level explanations. As the scale of the collaborative network expands, it becomes evident that many economies need to be more actively involved in the consideration and integration of collaborative efforts. The centrality of the network shifts as the level of threat heightens. Collaboration manifests at the meso level (medium systems) with organizations of a higher degree in the network, such as the WHO, which influence larger systems. The bigger the security threat, the higher the collaboration when the threat is more concentrated and known, such as AMR. A lesser-known threat, such as the novel coronavirus, raises (in)securities and concerns, reducing collaboration. However, macro-level threats affecting grander scales, such as economic issues, increase collaboration.

Phase 2: Qualitative Analysis of WHO-GLASS AMR Surveillance Case Study

The specific case study chosen for this research is the GLASS collaborative effort in AMR surveillance, led by the WHO. Data flows seamlessly through the network as actors share AMR surveillance information on platforms like GLASS, enabling timely responses to infectious disease threats. Actors create databases with the aim of "working within communities of practice, modes of governance, and technical constraints" (Kitchin 2014, 22). Platforms like GLASS exemplify how data sharing and technological integration transcend national boundaries to facilitate real-time monitoring and analysis. The GLASS's key objectives include collecting surveillance information to estimate the encumbrance of AMR, reporting global AMR data, and detecting the spread of emerging resistance to antimicrobials. This qualitative single case study also encompassed the IHR and infectious diseases since the boundary objects expand in scale and scope. Through network analysis, the social environment expresses patterns in relationships among interacting units (Wasserman and Faust 1994). Some actors use advanced technology databases as "the service of an action" to surveillance actants that are considered global threats (Bowker and Star 1999, 298). Infectious diseases serve as boundary objects because of the consequential nature of diseases in institutions, nation-states, and civil society.

Scholars consider infectious diseases a new threat to a nation's security and citizens. However, the concept of *new threats* historically addresses concerns focused on the role of the military following the end of the Cold War in addressing international military alliances and enemies (Saint-Pierre 2017). The regulations assist in mediating subsequent actions by actors since technological efficacy and social dynamics intertwine. Infectious diseases serve to mediate actor reactions in the network. Thus, the boundary objects communicate with multiple actors through collaboration and interconnectedness.

Moreover, any actor network is successful if it does not force potential actors to become its members (Balzacq and Cavelty 2016). The WHO, for example, does not force countries to participate and collaborate in the GLASS surveillance network. During an interview, the participation of Brazil in the GLASS system was discussed, and the interviewee's viewpoint was expressed in the following words: "It's not that the GLASS included Brazil. It's the other way around: Brazil enrolled in GLASS. It depends on the countries' willingness or not to enroll in GLASS" (confidential telephone interview with a team lead of antimicrobial drug resistance at the WHO, Geneva). Thus, although the countries voluntarily chose to use GLASS's standardized surveillance approach, the institution created an avenue of collaborative exchange through its communication platform in the connected ecosystem.

Institutions work toward resolving the global threat by joining the surveillance network, or through collaboration. Thus, the functions of ensuring national security and countering global threats in the form of pathogens fall into the legal realm through the IHR as an inscription device to transform facts into a regime. The international health regulations provided the rules and regulations to collaborate in GLASS (World Health Organization 2017b). The decision to contribute lies independently with the participating countries and the institution. However, interdependence co-exists amongst actors in a complex system to fight nonconventional threats.

Complex interdependence contributes to security governance during a collaboration of resources and data sharing between different actors, governments, and international organizations. While a collaborative factor exists amongst global countries to monitor pathogenic threats, some communities disrupt the initial premise. Rather than viewing such disruptive groups as not wanting to be part of the network, the disruption adds value to the development of the network. Without the bad, there is no righteous good. Likewise, the exponential growth of big data requires subject expertise and a command of computational techniques to "process, analyze and interpret this large-scale data" (Feng and Kirkley 2020, 1). Thus, diverse actors create a network prism of reality in promoting a health regime.

The situations in which an international organization, such as the WHO, raised the threat level for AMR include a high level of antibiotic consumption and the global rise of AMR. For instance, the World Economic Forum identified antibiotic resistance as a global risk unmanageable by any nation alone (World Health Organization 2015b; Howell 2013). Furthermore, a 2015 report in the WHA to develop a global action plan on AMR indicated that close to 100,000 Americans, 80,000 Chinese, and 25,000 Europeans die yearly from hospital-acquired antibiotic-resistant infections (Howell 2013). Likewise, over 700,000 deaths are attributable to AMR, projected to exceed 10 million, accompanied by a reduction of 2% to 3.5% in the gross domestic product (GDP) by 2050 (Aggarwal et al. 2023; O'Neill 2014). In addition, in 2016, world leaders gathered at the UN General Assembly in response to the growing threat of AMR. During the meeting, Dr. Marc Sprenger, director of the WHO's AMR Secretariat, noted that there have been "discussions of AMR in WHO since the 1960s, and plans since 2000, but it is now shifting from being a technical problem to a much higher-level political issue" (World Health Organization 2016c, 638).

The events that triggered the creation of GLASS go as far back as 2001 and can be traced to the initiative of the WHO global strategy to contain AMR (World Health Organization 2001) and the focus of the World Health Day in 2011 on AMR with the WHO issuing a six-point policy package calling for action by all global stakeholders (World Health Organization 2014). Through several resolutions, the WHA called for intensive implementation of the global strategy and strengthening of AMR surveillance. Testing for susceptibility to antimicrobials, which informs AMR surveillance, fell into the scope of the IHR, stipulating the requirement for access by states to the capacity to investigate any disease outbreak that could present an international public health threat (World Health Organization 2016a). Chapter 3 provides further analysis of the events that triggered the creation of GLASS since a harmonized system is needed to standardize the collection of official global AMR data. In 2014, the WHO created the first global report on national AMR surveillance for selected worldwide pathogenic bacteria that infect humans and examined the evidence base concerning the impact of AMR on health and the economy (World Health Organization 2014). Therefore, the results of the 2014 report led to the development of the global system, and in 2015, the WHO launched GLASS.

The scope of the present investigation included meetings with various actors to discuss the promotion of a health regime on monitoring communicable diseases and AMR surveillance. During the formation of the actor network, the fieldwork tracked information within the United States and other contributing actor contexts, particularly countries of the southern subcontinent of the Americas. The collaborations aimed to enhance surveillance of AMR and infectious diseases within the network. For instance, the second meeting in April 2014, with the Strategic and Technical Advisory Group for Antimicrobial Resistance (STAG-AMR), a principal advisory group to the WHO on AMR, attracted more than 30 participants: "representatives of intergovernmental organizations, civil society, public health and regulatory agencies, industry associations, professional organizations, and patient groups" (World Health Organization 2015b, 7). In December 2014, a global consultation by the WHO-GLASS brought together representatives of 30 member-states from the six regions of the WHO, international experts on AMR, and WHO staff (World Health Organization 2015c). In April 2017, the second high-level technical meeting on AMR surveillance included directors of ministries of health, GLASS-enrolled member-states, health regulatory agencies, epidemiologists, and WHO staff (World Health Organization 2017e). The meeting also included collaborating centers such as technical universities, public health schools, and communicable diseases institutes (World Health Organization 2017e). April 2021 saw the third high-level technical consultation and virtual meeting on AMR surveillance and the GLASS 2020 platform to generate evidence-based representable data for action (World Health Organization 2021d, 2020y). In addition to the actors previously mentioned, AMR technical surveillance officers, clinicians, partner institutions, and medical microbiologists from 21 of the 28 countries in the region of the Americas were also in attendance.

Moreover, during a meeting that determined the priority pathogens among antibiotic-resistant bacteria, the coordinating group in the meeting included experts in clinical microbiology, infectious diseases, public health, research and development (R&D), and infection control (World Health Organization 2017d). Furthermore, a group of 70 experts with diverse backgrounds and geographical origins in clinical microbiology, infectious diseases, public health and pharmaceutical R&D, and epidemiology was involved in the process of assigning appropriate criteria weights on the relevant importance of the selected bacteria for drawing up the list of priority pathogens (World Health Organization 2017d). The key goals of prioritizing pathogens include enabling the prioritization of R&D, spurring public and private funding, and expediting global strategies for R&D to uncover new antibacterial agents for the treatment of bacterial infections resistant to conventional drugs.

Furthermore, the criteria the experts looked at for each pathogen were arranged by the species and the type of resistance and the results stratified into three priority tiers (critical, high, and medium). Moreover, based on experience and previous prioritization exercises, nine criteria were selected to determine the level of threat (priority) of the pathogens: mortality, health care burden, prevalence of resistance, 10-year trend of resistance, community burden, transmissibility, preventability in community and health care setting, treatability, and pipeline (World Health Organization 2017d). The experts extracted evidence for the criteria from different sources, including systemic reviews of published literature, databases of European-financed projects, 23 national and international surveillance systems for antibiotic-resistant bacteria, and international guidelines on the prevention and treatment of infections due to antibiotic-resistant bacteria (World Health Organization 2017d).

To support the early implementation of GLASS covering the period 2015-2019, GLASS guided member-states in compiling standardized AMR surveillance data and sharing the information to form a global picture (World Health Organization 2015c). Furthermore, to optimize and prepare for the surveillance of AMR, the WHO organized a sequence of online technical discussions on AMR and antimicrobial user phases with the participating member-states. For instance, during the third high-level technical meeting on AMR surveillance, online technical discussions focused on strategies for disseminating and familiarizing national technical officers in charge of AMR surveillance with the GLASS technical documents (World Health Organization 2020y). In addition, the meeting familiarized national technical officers in charge of AMR with new technologies, such as metagenomics, and approaches to enhance AMR surveillance. The meeting also allowed sharing of experience within the WHO regions and between national technical officers from different countries. Likewise, the WHO-GLASS provided technical training on four themes: antimicrobial use and antimicrobial consumption methods, AMR surveillance methods, microbiology laboratory methods, and the One Health surveillance model (World Health Organization 2020y).

Moreover, leveraging the COVID-19 pandemic, the WHO regional office provided "remote guidance and training to national focal points from all member-states" to reinforce AMR surveillance (World Health Organization 2021d, 58). For instance, in the WHO region of the Americas, building on the ReLAVRA network, the regional office launched a training protocol on enhanced isolate-level AMR monitoring. Furthermore, a tripartite alliance of seven Latin American countries implemented the European-Union-funded project "Working Together to Combat AMR." As a result, the WHO regional office held "a series of ten online training sessions on the role of molecular biology in integrated AMR surveillance under the One Health approach" (World Health

Organization 2021d, 59). Also, the training included strengthening antimicrobial stewardship, teaching how to update their national essential medicine lists, and evidence-based selection of antimicrobials as well as providing the tools to develop a list of medicines essential for treating critical patients with suspected or confirmed COVID-19 (World Health Organization 2021d).

Similarly, in the WHO African region, in 2020, regional capacity was reinforced with five webinars that included a road map for coordinating and implementing global AMR surveillance. Likewise, support was provided to Togo to implement a mentorship project for bacteriology laboratories (World Health Organization 2021d), and in 2020, the CAESAR network organized a series of technical webinars and GLASS virtual consultations (World Health Organization 2021d). Another instance of international collaboration was "Implementation in seven countries (Burkina Faso, Cameroon, Ghana, Madagascar, Nigeria, Zambia, Zimbabwe) of the *E. coli* tricycle project surveillance system" (World Health Organization 2021d, 58). More recently, as of 2021, 13 countries took part in the enhanced isolate-level AMR surveillance phase through the ReLAVRA network, which enabled the countries to participate in GLASS: Ecuador, Argentina, Colombia, Chile, Costa Rica, Dominican Republic, Peru, El Salvador, Uruguay, Paraguay, Mexico, Trinidad and Tobago, and Belize (World Health Organization 2021d).

Likewise, the surveillance protocol in several countries from the Americas was enhanced to include *Candida* through the collaboration of the WHO Regional Office and the WHO Collaborating Center on AMR with the ANLIS Malbran Institute in Argentina and the WHO Collaborating Centre for Surveillance, Epidemiology, and Control of Foodborne Diseases and other Enteric Pathogens at the CDC. Thus, the international collaboration of actors in submitting AMR data to GLASS and adequate GLASS technical training on surveillance generated evidence-based action and preparedness at local and global levels. The remaining sections of this chapter provide further empirical analysis of international collaboration and the interconnectedness of actors in the surveillance of infectious diseases and AMR.

How are actors collaborating globally and conducting open information exchange on a surveillance platform? The early implementation stage of the GLASS database was from 2015 to 2019, which inspired a global collaborative effort on AMR surveillance (World Health Organization 2017b). In 2015, the WHO launched the GLASS for surveillance of bacterial pathogens specific to human beings. Part of the WHO's website, the GLASS provides formal and informal data across multiple platforms. The WHO referred to GLASS as the "first global collaborative effort to standardize AMR surveillance" (World Health Organization 2017b, 5). The sixty-eighth WHA endorsed GLASS through resolution WHA 68.7 (World Health Organization 2015b) and created GLASS to support the second objective of the WHO's Global Action Plan on AMR (GAP-AMR), namely, "to strengthen knowledge through surveillance and research" (World Health Organization 2015d, 127). The model makes it possible to conduct an insightful analysis of information from a given participating country as part of surveillance of communicable diseases. Each participating member-state[1] voluntarily enrolls in the GLASS, submits AMR data, and reports information into a data management software called WHONET (O'Brien and Stelling 1995). Dr. John Stelling, Associate Physician with the Brigham and Women's Hospital, Co-Director of the WHO Collaborating Centre for Surveillance of Antimicrobial Resistance, Developer of the WHONET software, stated on an interview on January 24, 2020, the "WHONET is now used in about 140 countries. We support indirectly maybe 3,500 labs or so, but we don't collect the data." The WHO receives aggregated information at the national level for review and also creates publicly available GLASS reports based on the aggregated statistics collected. Countries use the WHONET to prepare the GLASS submissions and the "WHONET analyzes the isolate level data to prepare national aggregate statistics shared with WHO" (interview with Dr. John Stelling, January 24, 2020). For instance, Ecuador's Ministry of Health and the Instituto Nacional de Investigación en Salud Pública (National Institute for Public

[1] This study uses the term member-states when describing participating countries' interaction with the WHO.

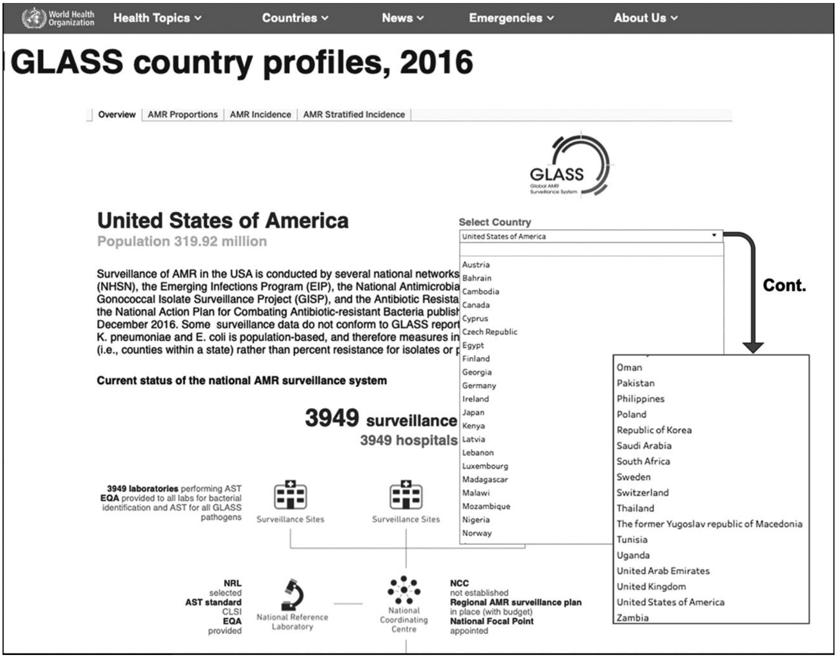
Health Research, INSPI for its initials in Spanish) utilizes the WHONET to monitor bacterial resistance in the country (Ministerio de Salud Pública del Ecuador 2019b). The WHONET contains datasets and algorithms for detecting outbreaks (Stelling et al. 2010), and Dr. John Stelling added that the WHONET is "using a software called SaTScan that looks to detect outbreaks." The software incorporates a visual map, spreadsheets, and statistics developed with close collaboration among the actors. Contributions from participating countries and NFP centers provide information to the database system. The surveillance network consists of three core components: an NCC, an NRL, and surveillance sites that collect epidemiological data and diagnostic results (World Health Organization 2017b). However, GLASS relies on the participating member-states to manage their national surveillance. Thus, structured heterogeneously, the data map countries and diverse actors voluntarily participating in the surveillance network.

The GLASS on the WHO-GLASS website provided country profiles with AMR data for 38 countries in 2016. Figure 3.12 shows the GLASS country profiles in 2016, displaying the countries available in the drop-down menu. It is important to note that the enrollment from South America is not included in these profiles.

Addressing potential discrepancies in open-source or publicly available information and considering concerns regarding the veracity of such data are crucial aspects. The findings of the study emphasize the necessity for comprehensive country profile overviews that address the challenges in identifying surveillance sites that contribute specimens to participating laboratories. An analysis was undertaken to discern the root causes, involving technical mishaps, administrative lapses in updating software, and delays in information submission by countries. The GLASS report indicated: "The identification of the total number of surveillance sites submitting specimens to participating laboratories was not possible due to the setup of the national surveillance system" (World Health Organization 2017b, 26). This limitation underscores the challenges in obtaining a complete picture of the contributions of the surveillance site to these laboratories.

Moreover, the information reveals that the United States was enrolled in GLASS in December 2016 but still needed to provide data to GLASS

Figure 3.12. Country profiles in 2016 from GLASS



Source: World Health Organization (2016d).

during this reporting period (World Health Organization 2017b). Likewise, in 2016, the GLASS platform database revealed that data from countries of the Global South had not been entered during this reporting period (see figure 3.12). In addition, the database indicated that among the GLASS country profiles listed in 2017, Brazil was enrolled in GLASS but unreported. Table 3.2 shows the number of countries enrolled in GLASS from 2017 to 2021 by data call.

From April 1 to July 8, 2017, the WHO-GLASS website launched its first data call (World Health Organization 2017b). During this initial data call, GLASS received 42 country enrollments, with only 40 countries submitting data on their AMR surveillance systems. By December 2017, there was a 19% increase (n = 50) in participating member-states enrolled

Table 3.2. Number of countries enrolled in GLASS from 2017 to 2021, by data call

Call by Global Antimicrobial Resistance and Use Surveillance System (GLASS) for data	No. of countries enrolled in GLASS	Date
None	109	May 2021
	107	Apr 2021
4th data call	94	Aug 2020
	92	Apr 2020
3rd data call	86	Oct 2019
	82	Jul 2019
2nd data call	71	Dec 2018
1st data call	50	Dec 2017
	42	Jul 2017 (End of first data call)

Source: GLASS reports, World Health Organization (2016–2021).

(World Health Organization 2017b). In addition, the research is not a controlled study since most countries provided incomplete data as judged by the standards of GLASS. However, the findings revealed that, during the preliminary stage, three of the BRICS[2] countries (India, Russia, and China), which are the main emerging national economies, were unlisted in 2017. Monitoring the GLASS website in January 2018 showed that 51 countries were enrolled. By May 2018, more than 25% of WHO-participating countries were enrolled in GLASS (n = 58), with 39 countries submitting AMR information. In 2018, Brazil was the only country from the southern subcontinent of the Americas enrolled in GLASS, but it did not report AMR data. By the end of the second call in July 2018, GLASS contained 69 enrolled member-states (World Health Organization 2018a); out of those, 67 submitted information on their surveillance systems, and 48 countries reported AMR data (World Health Organization 2018a). By December 2018, the number of participating countries that enrolled in GLASS had increased to 71, including the enrollment of two additional BRICS countries, India and Russia (World Health Organization 2018a). Does Russia

[2] BRICS is an acronym for Brazil, Russia, India, China, and South Africa.

and India's late entry into the GLASS system in 2018 change the context of the database and raise political awareness, especially concerning security? In 2018, GLASS revealed a "64% increase in country enrollment and more than twice the number of countries submitting AMR data" (World Health Organization 2018a, 5). At the end of the third data call in July 2019, the GLASS-AMR system contained 82 enrolled countries, with a 95% increase in enrollment compared to that in 2017 (World Health Organization 2020g) and included a second country from South America, Argentina. By October 2019, the enrollment had increased to 86, and a third country from South America, namely, Peru, appeared during this period. The GLASS enrollment by participating member-states had increased to 92 by April 2020 and to 94 by August 2020, although China continued to be unenrolled in the system (World Health Organization 2020g). By April 2021, GLASS enrollment had increased to 107, and within a month, "as of May 2021, 109 countries and territories worldwide had enrolled in GLASS" (World Health Organization 2021d, 4). Figure 3.13 shows the evolution of country participation in GLASS in 2018, 2019, 2020, and 2021. Thus, the number of collaborating countries increased during the period under study (2015-2021) and signifies increased knowledge production, awareness, and understanding of the urgency to combat global health threats.

Moreover, as the number of GLASS enrollments increased, the results showed that between 2015 and 2020, the HHS held 14 public meetings, one high-level meeting, and one listening session to discuss issues relating to combating antibiotic-resistant bacteria, including AMR. In 2020, out of the 14 meetings, the HHS held one public meeting and the one listening session on the problems of AMR and in the same year released the subsequent version of the "National Action Plan for Combating Antibiotic-Resistant Bacteria" (ASPE 2020). Out of the two events held in 2020, the HHS organized a virtual meeting focused on COVID-19 and AMR.

Based on the data collected from 2015 to 2021, the study examined the interactions between actors enrolled in the GLASS platform and actors outside the platform who were relevant to the surveillance and security governance of infectious diseases. This analysis aimed to illustrate the interconnectedness and collaboration among these actors in addressing the challenges of infectious disease surveillance. For example, in February and September 2020, meetings were held by the HHS through the PACCARB: the listening session in February discussed the landscape of AMR, and the

Figure 3.13. Number of countries enrolled in GLASS: 2018-2021

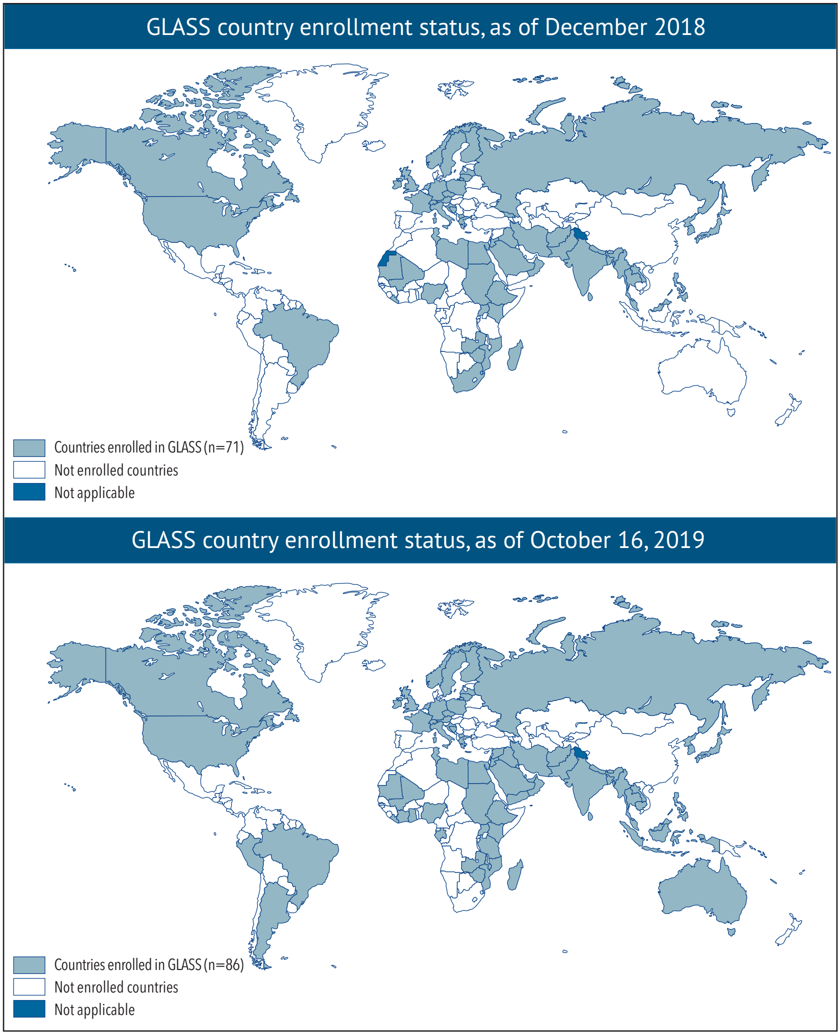
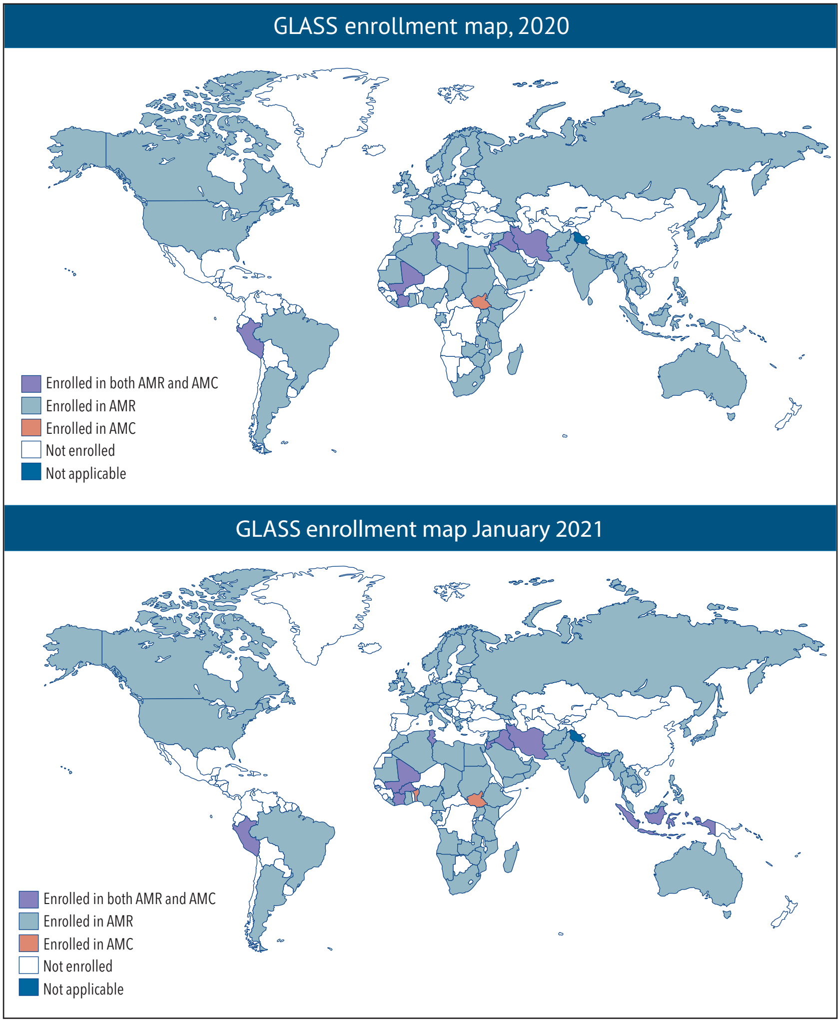


Figure 3.13. (*continued*)



Source: Geographic information, World Health Organization (2018-2021).

public meeting in September discussed in its agenda the impact of coronavirus infectious disease (COVID-19) on AMR (U.S. Department of Health & Human Services 2020b, 2020a). Decision-making units, such as a nation-state, perceive threats even when they decide to operate in a regional cooperation regime to guarantee the security and well-being of their citizens (Saint-Pierre 2017). However, not all countries cooperate so readily due to socioeconomic, historical, or political conflicts. Under the cooperation, actors change their behaviors depending on the behaviors of other country or countries. Meanwhile, security measures, rules, or protocols answer the call to collaboration. For instance, from 2015 to 2021, GLASS-participating countries maintained steady collaboration on the well-known issue of AMR.

As the novel threat, COVID-19, entered the landscape, fears and uncertainty increased, leading to a decrease in global cooperation while increasing collaboration for countering the threats of AMR and COVID-19. In April 2020, a group of global health and private actors launched a landmark collaborative action committing to proactively engage stakeholders, align efforts, build collaboration, and devise transparent solutions grounded in science (World Health Organization 2020d). In 2021, the Group of Friends on Tackling AMR launched a call to action to raise global efforts to address AMR, which included 113 member-state signatories, including Argentina, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay, and Venezuela, and 38 supporting organizations (World Health Organization 2021b). Similarly, an observational review was conducted in September 2020 during an official virtual meeting organized by PACCARB on the topic of AMR and COVID-19 (U.S. Department of Health & Human Services 2020a). A diverse mix of private and public actors was present during the PACCARB meeting, including 15 voting members, 8 organizational liaisons, 11 regular government employees, one designated federal official, and two advisory council staff (U.S. Department of Health & Human Services 2020a).

Moreover, data collection and analysis on COVID-19 were incorporated as an additional source of information to examine the collaborative network of actors within the Gephi quantitative network analysis framework. A document review and analysis conducted using the WHO SITREP revealed the collaborative efforts of actors and the engagement of countries in COVID-19 surveillance efforts. Table 3.3 illustrates the surveillance of

COVID-19 and the collaboration of nation-states in reporting their total confirmed cases of COVID-19 in 2020 and 2021. The table concentrates on the United States and South America from the beginning of the outbreak until one year later, in 2021, and shows when each country first reported cases of the coronavirus disease and how the outbreak quickly spread within a year. The table also shows when each country first reported a covid case (cells shaded gray). Brazil and the United States were the first countries from the northern and southern subcontinents of the Americas to report cases of the coronavirus disease. Within the first week of March 2020, five more South American countries–Ecuador, Argentina, Chile, Colombia, and Peru–reported their first cases of COVID-19 (World Health Organization 2020j, 2020k, 2020l, 2020m), followed by the remaining countries in the region (World Health Organization 2020n, 2020o, 2020p, 2020q, 2020r).

By July 31, 2020, the WHO had reported 17 million confirmed cases of COVID-19 (World Health Organization 2020s), and as of December 27, 2020, the number had crossed 79.2 million (World Health Organization 2020f). On February 21, 2021, one year after the first confirmed cases in March 2020, the WHO reported over 111 million global confirmed COVID-19 cases (World Health Organization 2021c). By July 25, 2021, the number was 194 million and, as of October 24, 2021, 243 million (World Health Organization 2021e, 2021f). The pandemic conditions provided a more urgent opportunity for nation-states to establish appropriate practices and implement security measures in response to the COVID-19 virus while also addressing concerns related to AMR. Although the AMR shown by bacterial pathogens of human importance remained a focus for health authorities and health officials, the COVID-19 pandemic attracted immediate attention across country borders. Nonetheless, despite the challenges that the COVID-19 pandemic presents to health systems and AMR surveillance, "countries were able to maintain their capacity to detect and rapidly alert to any AMR threats of public health importance" (World Health Organization 2021d, 59).

In conclusion, this section focused on the qualitative analysis of GLASS and infectious diseases as boundary objects through interviews

Table 3.3. Confirmed cases of COVID-19 in the Americas (2020–2021)

Country	Outbreak									Mid-Year	Year end	1 year mark
	Feb-27-20	Mar-1-20	Mar-4-20	Mar-7-20	Mar-9-20	Mar-11-20	Mar-13-20	Mar-14-20	Mar-16-20	Jul-31-20	Dec-27-20	Feb-21-21
U. S.	59	61	108	213	213	696	1264	1678	1678	4,388,566	18,648,989	27,702,074
Brazil	1	2	2	13	25	34	77	98	200	2,555,265	7,448,560	10,081,676
Colombia	-	-		1	1	3	9	16	24	276,055	1,574,707	2,217,001
Argentina	-	-	1	2	12	17	31	34	56	178,996	1,574,554	2,054,681
Peru	-	-		1	6	11	22	28	71	400,683	1,005,546	1,269,523
Chile	-	-	1	5	10	17	33	43	75	353,536	598,394	795,845
Ecuador	-	1	7	14	15	15	17	23	37	83,370	209,274	273,097
Bolivia	-	-	-	-	-	2	3	3	11	73,534	153,590	240,676
Paraguay	-	-	-	-	1	5	5	6	8	4,866	103,888	149,684
Venezuela	-	-	-	-	-	-	-	2	2	17,159	111,603	135,114
Uruguay	-	-	-	-	-	-	-	-	4	1,237	15,848	51,377
Suriname	-	-	-	-	-	-	-	-	1	1,607	5,880	8,854
Guyana	-	-	-	-	-	-	1	1	4	398	6,289	8,357
Total North America	59	61	108	213	213	696	1,264	1,678	1,678	4,388,566	18,648,989	27,702,074
Total South America	1	3	11	36	70	104	198	254	493	3,946,706	12,808,133	17,285,885
No. of SITREPs	**38**	**41**	**44**	**47**	**49**	**51**	**53**	**54**	**56**	**193**	**Weekly SITREP**	**Weekly SITREP**

Source: WHO situation reports (2020–2021).

and document analysis. The qualitative data structure frames the procedure of the philosophical theories chosen in this study. Furthermore, the qualitative information connects to various disciplines and provides some understanding and explanation to enhance the results from analyzing quantitative data. Thus, combining two distinct datasets–qualitative and quantitative–allows a movement beyond traditional statistical analysis toward a kaleidoscope of integrated and comprehensive data.

This research included discourse on using ideas and knowledge of diverse experts from the scientific, security, intelligence, health, military, and academic disciplines. These relevant actors are vital to the process of providing support pertinent to the core of the system. Subsequent chapters also include commentaries from various interviewees. The following section on GLASS-selected pathogens and surveillance of AMR, the security governance metrics framework, and the five dimensions of security governance enables us to answer the research question in greater detail.

From Antimicrobial Resistance to COVID-19

In early 2022, the virus continued to cross oceans when individuals had to deal with a deadly pandemic and partisan divisions. At one end, the novel coronavirus continued to spread over wider areas; at the other, actors tackled another emerging pandemic, AMR. Therefore, infectious diseases continued to span oceans and borders, whether known or unknown. This section includes a description of the GLASS database, a discussion of infectious diseases, such as those caused by the eight bacterial pathogens, and a brief discussion of the COVID-19 coronavirus.

The WHO published a report in 2014 as a first look, from a global perspective, at antibacterial resistance (ABR) and surveillance of AMR in common bacterial pathogens (World Health Organization 2014) in collaboration with member-states and partners across different sectors. Antibiotic resistance pertains to strains of microorganisms that develop resistance to antibiotics: AMR occurs when microorganisms such as viruses, bacteria, parasites, and fungi acquire resistance to an antimicrobial medicine to which they were previously sensitive (World Health Organization 2015c; O'Toole 2013). Thus, ABR occurs when bacteria develop resistance to an antibiotic. The report served as the baseline to measure data on pathogens and strengthen the collaboration on AMR surveillance. Therefore, the report, which included ABR information, served as the starting point for the modern GLASS framework integrating AMR data from other areas such as animal-human interface, environmental AMR, and consumption of antimicrobials.

The data presented by GLASS were reported through a customized software, namely, the WHONET. The system obtains information from GLASS-enrolled countries for individuals interested in studying or learning about the surveillance of antimicrobials that infect human beings. The WHO established a priority list of pathogens, including two coronaviruses, namely, the Middle East respiratory syndrome coronavirus (MERS-CoV) (de Groot et al. 2013) and the severe acute respiratory syndrome (SARS) (World Health Organization 2017d, 2017c). Although many other bacterial pathogens exist, the surveillance system focused on eight pathogens. In 2015, the WHO developed a surveillance system for them, and GLASS reports on the following bacteria that cause common hospital and community-acquired infections globally: *Acinetobacter* spp. (*Acinetobacter*), *Escherichia coli* (*E. coli*), *Klebsiella pneumoniae (Klebsiella), Neisseria gonorrhoeae* (*N. gonorrhoeae*), *Salmonella* spp. *(Salmonella)*, *Shigella* spp. (*Shigella*), *Staphylococcus aureus* (*S. aureus*), and *Streptococcus pneumoniae* (*S. pneumoniae*) (World Health Organization 2017b). The WHO listed global pathogens that carry a priority, which includes the above eight pathogens (World Health Organization 2017d, 2017c). Table 3.4 lists the pathogens in order of priority and the type of resistance (World Health Organization 2017c, 5). A team of experts drawn from public health and pharmaceutical R&D, epidemiology, infectious diseases, and clinical microbiology selected the bacteria to be prioritized into three tiers: critical [1], high [2], and medium [3] (World Health Organization 2017c).

Whereas other global surveillance systems already produce data on infectious diseases such as tuberculosis, malaria, HIV, and influenza and on

Table 3.4. Pathogens accorded priority by the WHO and their resistance to antibiotics

Priority	Pathogen	Antibiotics to which the pathogen is resistant
1	*Acinetobacter baumannii*	Carbapenem
1	*Escherichia coli*	Carbapenem and third-generation cephalosporin
1	*Klebsiella pneumoniae*	Carbapenem and third-generation cephalosporin
2	*Staphylococcus aureus*	Methicillin and vancomycin
2	*Neisseria gonorrhoeae*	Third-generation cephalosporin and fluoroquinolone
2	*Salmonella* spp.	Fluoroquinolone
3	*Shigella* spp.	Fluoroquinolone
3	*Streptococcus pneumoniae*	Not susceptible to penicillin

Source: Prepared by the author using data from the WHO.

drug resistance, the WHO-GLASS team chose the eight pathogens to complement the effort. As an interviewee indicated,

Team lead of antimicrobial drug resistance. The idea of including only specifically known bacterial pathogens was based on the fact that other surveillance systems already existed for monitoring other types of pathogens, viral pathogens, parasitic pathogens and tuberculosis. So, there is no prejudice against any other global threat, but to fill a gap that at the time we have seen (confidential telephone interview at the WHO, Geneva).

The bacterium *Acinetobacter* is found in water and contains opportunistic species that can cause diseases (O'Toole 2013): *A. baumannii* causes such diseases as pneumonia, wound infections, bacteremia, and meningitis (O'Toole 2013). The genus *Acinetobacter* contains many species between the non-baumannii group and the *Acinetobacter* baumannii group, which consists of *A. pitti*, *A. baumannii*, and *A. nosocomialis* (World Health Organization 2017b). Immunocompromised individuals are most at risk from infection, mainly inside health care settings and intensive care units (Brady, Jamal, and Pervin 2021; O'Toole 2013). *Acinetobacter* is resistant to many antimicrobial agents because of its "selective ability to exclude various molecules from penetrating their outer membrane" (World Health Organization 2017b, 139). Nevertheless, the organism colonizes tissues in patients that do not have symptoms and exist in open wounds, such as an opening in front of the neck following tracheostomy (O'Toole 2013).

The bacterium *E. coli*, commonly present in milk, water, soil, and the intestines, causes "urinary tract infections, pneumonia, bacteremia, and peritonitis, among others" (Mueller and Tainter 2021, sec. 3, para. 1; O'Toole 2013). In addition, blood poisoning caused by the bacteria quickly leads to shock or death of the individual (O'Toole 2013). More specifically, *E. coli* frequently causes community and hospital-acquired urinary tract infections and infections of the kidney and neonate meningitis and is one of the leading causes of global foodborne infections (World Health Organization 2017b). Furthermore, although infections from *E. coli* derive from the gut of the affected individual, AMR strains are transmitted from animals and spread between individuals (World Health Organization 2017b). Likewise, despite carbapenems remaining an available treatment option for severe infections such as *E. coli*, the WHO notes that "carbapenem resistance in *E. coli* is an emerging threat" (World Health Organization 2017b, 139). Thus, the WHO classified carbapenem on the priority list of AMR and considered *E. coli* a high-risk species that causes complications such as developing life-threatening kidney failure.

Species of *Klebsiella* bacteria exist in cereal grains, water, soil, animals, and the human intestinal tract and are associated with pathological conditions such as pneumonia (O'Toole 2013). Diseases that result from *Klebsiella* include infections of the bloodstream, urinary tract, and lower respiratory tract, with the majority of human infections caused in a health care setting (World Health Organization 2017b). In addition, *Klebsiella* contains a resistance gene that renders penicillin ineffective and is the leading global cause of infections caused by carbapenem-resistant bacteria (World Health Organization 2017b).

The next priority pathogen is *N. gonorrhoeae*, which causes gonorrhea, an acute sexually transmitted infection (Wi et al. 2017; O'Toole 2013). The WHO noted that not treating the infection results in severe complications, such as inflammation in the reproductive and genital tracts leading to further damage and infertility (World Health Organization 2017b). In addition, *N. gonorrhoeae* also infects parts of the gastrointestinal tract, such as the rectum, and pharynx. Resistance to antimicrobials counters the treatment of gonorrhea, causing the pathogen to evolve into a superbug. The study shows the likelihood that the global issue of the resistance of *N. gonorrhoeae* to antibiotics will worsen in the foreseeable future, and "the severe complications of gonorrhoea will emerge as a silent epidemic" (World Health Organization 2017b, 140). Thus, the WHO placed *N. gonorrhoeae* and its resistance to antimicrobials on the high-priority list to monitor, research, and develop an effective treatment.

Ingesting contaminated water or food or through person-to-person contact transmits the pathogenic *Shigella*, which causes gastroenteritis or diarrhea (World Health Organization 2017b; Wi et al. 2017; O'Toole 2013). Although patients recover within approximately seven days of contracting the disease, "shigellosis can be a life-threatening or fatal disease, particularly in children" (World Health Organization 2017b, 141). A growing concern is the gaps in information at the national level and inadequate reliability of local data to inform the appropriate treatment. Therefore, due to a minimal recovery period, the WHO placed *Shigella* and fluoroquinolone AMR in the medium tier in the priority list to develop advanced and effective treatments.

Species of Salmonella "include species causing typhoid fever, paratyphoid fever, and some forms of gastroenteritis" and are widely distributed in animals, producing a disease that transfers to humans and results in food poisoning (O'Toole 2013, 1591). *Salmonella* infection arises through the consumption of contaminated water, food, or beverages. For example, a foodborne outbreak occurs when animal or human feces contaminate the surface of foods (World Health Organization 2017b). Strains of *Salmonella resistant to multiple drugs* have emerged worldwide, and fluoroquinolones have been used for treating the disease. However, the "multidrug resistant *Salmonella enterica* serotype Typhimurium has been associated with a higher risk of invasive infection, higher frequency and duration of hospitalization, long illness, and increased risk of death" (World Health Organization 2017b, 141). Therefore, due to treatment failure, the WHO listed fluoroquinolone-resistant *Salmonella* on the priority list in the higher tier to develop better treatments of antibiotics.

The infectious pathogen *S. pneumoniae* causes community-acquired pneumonia and other human maladies worldwide (Dion and Ashurst 2021; O'Toole 2013). The cost to hospitalize patients with community-acquired pneumonia in the United States amounts to approximately $9 billion a year, with 22% mortality. It is the leading cause of death in all infectious diseases (Dion and Ashurst 2021). The pathogen also causes other diseases, such as infection of the middle ear (acute otitis media), infection in the bloodstream, and meningitis. Therefore, the WHO classified penicillin-non-susceptible *S. pneumoniae* as a medium priority tier in R&D for novel treatment.

The pathogen *S. aureus* is of global concern because of its resistance to antibiotics and is generally found on the nose or skin of healthy individuals and is "responsible for a number of pyogenic infections, such as boils, carbuncles, and abscesses" (O'Toole 2013, 1685). In addition, the pathogen produces toxins that cause symptoms such as food poisoning and toxic shock syndrome (World Health Organization 2017b) and causes a broad spectrum of clinical infections, which result in the direct invasion by bacteria of organs and tissue. The infection results in the "release of various toxins, either locally or systematically, and include[s] a range of diseases dependent on the location of the infection" (Zurita, Mejía, and Guzmán-Blanco 2010, S98). The pathogen lingers as a challenge because of multi-drug-resistant strains such as methicillin-resistant *Staphylococcus aureus* (MRSA) (Taylor and Unakal 2021), a particular "growing problem across Latin America" (Zurita, Mejía, and Guzmán-Blanco 2010, S97). In addition, MRSA presents cases of asymptomatic carriage. According to the CDC, "approximately 5% of patients in the U.S. hospitals carry MRSA in their nose or on their skin" (CDC 2019b, para. 4). Long-time cases of MRSA colonization or infection last from approximately 260 days to 40 months (Scanvic et al. 2001), and asymptomatic carriers transmit MRSA (Worby et al. 2013). Although community-acquired MRSA has been on the increase in many countries, some antibiotics can control the strains of MRSA. However, more complex multi-drug-resistant strains continue to cause health-care-associated MRSA infections (World Health Organization 2017b). Therefore, the WHO listed *S. aureus* and AMR to methicillin and vancomycin on the high-priority list to develop further treatments.

In 2018, the WHO revisited the original priority list and added Zika virus and Disease X, the latter referring to any new unknown virus that causes an epidemic. In 2019, an unknown virus appeared, and the medical community ruled out MERS, SARS, and influenza. A novel global virus threat had emerged: COVID-19. The rapidly growing outbreak of COVID-19 was derived from the etiologic agent, severe acute respiratory syndrome coronavirus (SARS-CoV-2), which, according to the WHO, began in Wuhan city in China's Hubei province (World Health Organization 2020h; Sanche et al. 2020). On December 31, 2019, Wuhan City reported several cases of unknown etiology (World Health Organization 2020t), and within the timeframe of this study, from December 31, 2019, to January 3, 2020, the WHO reported 44 cases of pneumonia from as yet unknown cause in China (World Health Organization 2020h). The virus belonged to the new coronavirus family in what the medical community temporarily called 2019-nCoV. On January 27, 2020, the Secretary of the U.S. Health and Human Services, Alex M. Azar II, determined that a public health emergency existed (U.S. Department of Health & Human Services 2020c), and the WHO declared COVID-19 as an "outbreak to be a public health emergency of international concern" (World Health Organization 2020i). By January 31, 2020, the WHO had reported a total of 9826 confirmed cases of COVID-19 worldwide (World Health Organization 2020i). On February 11, 2020, the WHO officially designated the virus as the coronavirus disease 2019 (COVID-19) (World Health Organization 2020x, 2020v). In March 2020, the WHO declared the virus as a pandemic (World Health Organization 2020w), elevating COVID-19 to the priority list of infectious diseases. Subsequently, the disease rapidly transcended national borders, becoming a global pandemic by mid-2020.

The investigation notes that the WHO-GLASS does not include COVID-19 surveillance data among the data on the eight bacterial pathogens that infect human beings and are listed during the implementation stage because the virus was outside the parameters of the GLASS architecture. Furthermore, when asked about the coronavirus and its connection to the GLASS surveillance of infectious diseases, a WHO interviewee remarked, “GLASS is about global surveillance of AMR, and it’s outside the scope of GLASS” (confidential telephone interview with a team leader of antimicrobial drug resistance at the WHO in Geneva). Therefore, the coronavirus occurred outside the realm of the selected GLASS pathogens.

How does the COVID-19 infectious disease shape reaction and response to the slow-moving but no less deadly looming threat of untreatable bacterial infections, the silent AMR pandemic? Even though COVID-19 does not fall within GLASS, the WHO official added that it is relevant to this study because of the “link across several surveillance systems at a higher level for public health purpose of each governing body in charge of looking at infectious disease burden” (confidential telephone interview with a team lead of antimicrobial drug resistance at the WHO, Geneva). Moreover, many surveillance systems of infectious diseases connect on health information because of the nature of global public health and the safety and well-being of civil society. Therefore, this case study includes information on COVID-19 as contextual evidence and a reinforcement mechanism.

Moreover, since the WHO considers AMR a critical global public health problem deriving from resistance to medicines used for treating infectious diseases (World Health Organization 2020b, 2017b), the COVID-19 pandemic also complicated human and national security as a global public health crisis and slowed down R&D in many industries, including AMR surveillance. Therefore, infectious diseases such as the coronavirus remain the focus of attention for health authorities and decision-makers.

There is a difference in threat level between a bacterial infection that cannot be treated with medicines (because of AMR) and the COVID-19 viral illness, against which antibiotics are ineffective. Nevertheless, the pandemic has had “a substantial impact on health systems globally, affecting the management of other health threats, such as antimicrobial resistance (AMR)” (Tomczyk et al. 2021, 3046). Moreover, after more than two years of tackling COVID-19, the threat of AMR is “not only still present but has become an even more prominent threat” (CDC 2022c, 3). For instance, in

2020, in a health care setting, the "bacterial nosocomial infections were more common in COVID-19 patients," and the most frequent bacteria identified as a percentage of all true bacterial tests in patients with COVID-19 were *S. aureus*, *Klebsiella*, and *E. coli* (Scott et al. 2022, 3). In addition, the CDC identified substantial increase in infections in health-care-associated pathogens such as *Acinetobacter* (CDC 2022c). Therefore, bacterial superinfection occurred in many COVID-19 patients and enhanced the relevance of the study in connection with infectious diseases.

On the one hand, COVID-19 "results in a wide spectrum of disease from asymptomatic carriers through pneumonia, acute respiratory distress syndrome (ARDS) and death leading to many hospitalizations and ICU admissions" (Scott et al. 2022, 1). On the other hand, analysis of the data reveals that bacterial pathogens pose a threat and have been the cause of a disproportionate number of human deaths and diseases. Therefore, public health systems should prepare themselves to fight multiple threats simultaneously.

Various threat levels of infectious diseases coexist, and the connection between (a) surveillance networks in different fields and threat entities and (b) the drive for open information sharing helps to know when global health is on the rise and to arrive at an informed response to the outbreak. In addressing one primary disease, states and institutions such as the WHO collaborate with different actors to target other infectious diseases. In addition, COVID-19 led to a need for more research on combating infectious diseases across many industries, including AMR. Thus, its impact after the scope of the case study and post-pandemic has been detrimental to global health policy matters.

Neglecting the audience for valuable information on an infectious disease that caused a global pandemic, and its influence on response, preparedness, research, and development of AMR and other bacterial pathogens, would be unwise. This study emphasizes the importance of knowledge production and data sharing to address complex issues effectively. Currently, COVID-19 represents a major threat, while AMR is considered a minor threat, silently lurking in the background. However, both are equally significant in promoting a health regime. Thus, to prevent a pandemic caused by an antimicrobial-resistant pathogen, it is crucial to identify gaps by examining the collaboration and interconnectedness of actors in the network, including variables such as COVID-19, which has reshaped the world.

COVID-19, like AMR, represents a complex and system-wide public health concern for which comprehensive solutions are needed. Relying solely on individual factors, such as therapeutics, public behavior, diagnostics, vaccines, or surveillance, will not be sufficient. Instead, a combination of all these elements is crucial for making progress and finding solutions. Antimicrobial resistance is projected to become the next pandemic following COVID-19, albeit with a slower but equally lethal impact over the long term. It poses a threat to safe health care delivery and has the potential to significantly impact global research, treatment, and development efforts, necessitating sustained collaborative responses across multiple sectors and geographical regions. Addressing drug resistance and infections requires the collective action of many nation-states, actors, and stakeholders. The analysis of both AMR and COVID-19 holds high value and serves as an important example of preparedness for future threats. This study focuses on AMR but also incorporates COVID-19 data, providing vital insights into interventions, preparedness, and interconnections. Thus, the coronavirus serves as a modern-day contextual research element and reinforces the findings of this investigation.

Likewise, new issues and contemporary threats inspire discourse and analysis in the decision-making process since cyberspace consists of many spaces (Balzacq and Cavelty 2016; Fontaine 2015). Moreover, science and technology contribute to addressing the intractable problem of disentangling the impossible knot and navigating the concept of the network, often referred to as the Gordian knot (Balzacq and Cavelty 2016; Latour 1993). Delegates of the WHO and participating countries collaborated in implementing the IHR, wherein networks, previously voiceless, now play a significant role. The interplay between the orderings of nature and society allows changes in external truth and legal subjects without overlooking the co-production of science and society (Jasanoff 2004; Latour 1993). Representatives, acting on behalf of the state, emphasize the crucial roles of actors, courses of action, and instruments in this intricate, global, and complex landscape (Jasanoff 2004; Latour 1993). Control in this context is intricately linked to knowledge infrastructure and to the question of "who has the right to speak in the name of science" (Bowker 2001, 7). Thus, a network ceases to function effectively when information from actors proves to be irrelevant to the network. Therefore, the interweaving of science and technology with the elements of nature and society creates a complex quilt of social tasks and necessitates heightened security measures.

International collaboration includes the unique leadership role of stakeholders from private to public-sector actors contributing to collaborative efforts, including open data sharing and actions leading to preparedness in anticipation of the pandemic. Governmental instruments facilitate collaboration to enhance public health and address nontraditional and global security threats. How can we incentivize bottom-up approaches to align with the continuous production of knowledge and information strategies? Strengthening relationships at the highest levels involves lateral interconnections across multiple industry sectors, incentivizing the surveillance of infectious diseases, and managing data security, with effects cascading down to the grassroots. The virus disregards geographical borders and shows no regard for national boundaries. Barriers are ineffective against the spread of the virus. Thus, fostering international relationships becomes imperative.

Measuring Security Governance to Promote a Health Regime

The present research establishes a metrics framework for security governance aimed at assessing the effectiveness of security governance in controlling diseases and managing data exchange during the surveillance of infectious diseases to promote a health regime. The study examines security governance by evaluating the perception of nonconventional threats and aims to answer questions such as how to measure security governance and what factors contribute to its success or failure. In order to evaluate the effectiveness of security governance in open data sharing within the GLASS system for infectious disease surveillance, the study focuses on understanding the operational aspects of the GLASS network.

More specifically, where views on governance arise as the "sum of the many ways individuals and institutions, public and private, manage their common affairs" (Webber et al. 2004, 5), the study looks to the performance and reliability of the GLASS network and interactions between relevant actors. Fundamentally, in what ways do we have privacy? Does privacy even still exist? While technology continues to develop, how do actors maintain a modicum of privacy in our elementary activities? Have we lost the right to control the information that robust computing systems gather on our lives? As users of information, "openness, transparency, and fair use of personal data should be rights to us" (National Academies of Sciences Engineering and Medicine 2015, 6). Nevertheless, the data controller decides how and in what form to process data and shares an element of dominion that blankets openly available information.

The crucial concerns deal with the wedding of the WHO and algorithms originating from the WHONET imported into the GLASS results. Furthermore, the data enable the WHO, its practices, and algorithms to track the surveillance on AMR and bacterial pathogens. In this instance, "countries provide AMR data primarily for pathogens isolated from blood specimens, followed by urine, stool, cervical and urethras ones" (World Health Organization 2017b, 6). Does the WHO-GLASS network, including the WHONET technology, adequately protect the organizational process it purports to protect? In order to develop measures for security governance activities, careful consideration was given to communication efforts and the intended audience. This research specifically targets science, technology, and security leaders who are responsible for an organization's operational, technological, and compliance aspects. The aim is to analyze security governance from their perspective and understand how they perceive and approach the subject.

This study examines the perspectives of security and privacy experts in the health care industry, focusing on leaders seeking to enhance the effectiveness of service delivery capabilities through the evaluation of processes, technology, and compliance measures. While earlier chapters established the theoretical and methodological foundations, this section extends the analysis by evaluating the practical implications of the WHO-GLASS network, particularly its AMR surveillance system, in the delivery and exchange of critical information among member states. This progression aligns with the structured exploration of the research question, ensuring a logical flow from conceptual frameworks to applied case study findings.

The methodology to create the metrics includes measuring the perception of nonconventional threats. John P. Pironti's approach (2007) to metrics of information security inspires this research. This study develops the measurements by establishing a baseline framework of metrics. Following Pironti's approach, the initial blueprint for this study was developed as the baseline framework of security governance, shown in figure 3.13. This framework serves as a foundation for understanding and analyzing various aspects of security governance within the context of the research. After establishing the baseline framework for each element, the study populates subcategories that account for "audience- and concept-specific metrics" (Pironti 2007, 2), as seen in the framework of the metrics of security governance (figure 3.14). These subcategories include operational, technological, and compliance metrics.

Pironti (2007) introduced operational, technological, and compliance metrics that address the implementation of security controls and

Figure 3.14. Baseline metrics framework

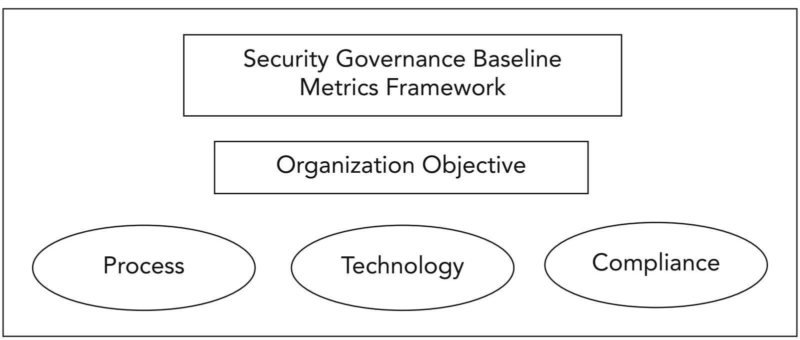
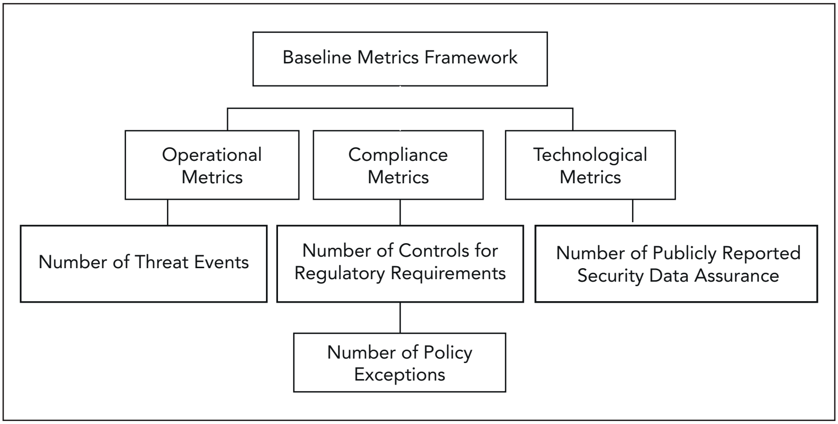


Figure 3.15. Security governance metrics framework



processes at the program and systems level. Consequently, the focus of this study centers on these three metrics, as they are closely aligned with the central research question: Why did security governance through an open technology database of the WHO contribute to a health regime for the surveillance of infectious diseases in the Americas between 2015 and 2021? As such, this research selects the three taxonomies that are most suitable for the study.

The focus was on the principal goals of the technology database when formulating the three metrics. The WHONET aims to enhance local utilization of laboratory data, facilitate global collaboration through data sharing, and "support the WHO goal of global surveillance of bacterial resistance to antimicrobial agents" (O'Brien and Stelling 1995, 66). With these objectives in mind, metrics were developed to establish security governance in disease control and data management during information exchange. The implementation of various metric tools in the surveillance of infectious diseases fosters a health regime. Therefore, these metrics serve as the foundational elements for security governance, a concept further reinforced in the subsequent section of the case study analysis.

Managing Security Threat: Operational Control of Infectious Diseases Through a Surveillance Network

How did the WHO-GLASS network function in the control of infectious diseases? Within the realm of operational metrics, the number of threat incidents on the GLASS platform was monitored from 2015 to 2021 to assess the effectiveness of the institution's operational control over infectious diseases. The examination of operational metrics sought to determine whether the WHO-GLASS framework encompassed disease management throughout its operational process. The ability of the actors involved to oversee the surveillance operation by monitoring the frequency of microorganisms signifies operational control as a security measure against a threat. Consequently, this proactive control contributes to an elevated level of security, which guides international surveillance of the threat.

Since different countries submit information on national AMR surveillance, a limitation of the study includes the complexity of comparing results by region or by country. For instance, GLASS notes the impracticality of comparing 2017 data with 2018 data to monitor progress within regions since each country submitted data at different periods across the five-year scope of the study. For example, drawing on data from the first GLASS data call in 2017, the study shows the selected priority bacteria that cause human infections in the Americas region (see table 3.5). The results illustrate the top pathogens, including *N. gonorrhoeae* and *Salmonella* spp., that present global public health threats to countries in the Latin American region.

Whereas table 3.5 shows a few countries of the Americas reporting on AMR pathogens (n = 3), the participation of member-states illustrates the process of controlling and monitoring infectious diseases by submitting AMR data in the surveillance network. Likewise, the study shows other countries reporting AMR data, with 3,097 hospitals and 2,358 outpatient clinics reporting to GLASS (World Health Organization 2018a). Furthermore, according to the GLASS 2017-2018 report, "45 (94%) countries submitted results from blood specimens, 24 (50%) from urine specimens, 21 (44%) from stool specimens, and 20 (42%) from cervical and urethral specimens" (World Health Organization 2018a, 15). Thus, the

Table 3.5. Number of countries in the Americas region reporting data, by source of specimens and specific pathogens in 2017

Americas Region AMR Surveillance of Public Health Threat Selected Priority Bacteria								
Source of specimens	Pathogens							
n = 3	*Acinetobacter*	*E. coli*	*Klebsiella*	*N. gonorrhoeae*	*Salmonella*	*Shigella*	*S. aureus*	*S. pneumonia*
Blood	X	X	X	X	1	X	X	X
Genital	X	X	X	1	X	X	X	X
Stool	X	X	X	X	1	X	X	X
Urine	X	X	X	X	X	X	X	X

Source: World Health Organization (2018a).

study shows that although only three countries from the Americas reported pathogenic AMR activity between 2017 and 2018, the total number of patients with suspected infection by an isolated pathogen reached a maximum of 859,002 patients per country (World Health Organization 2018a). Furthermore, according to the GLASS results, the two pathogens most frequently reported between 2017 and 2018 by participating member-states in South America were *N. gonorrhoeae* and *Salmonella* spp. Thus, AMR surveillance of these infectious diseases generated perceptions of a global threat to public health in the region.

Moreover, other countries in South America focused on AMR monitoring through PAHO, which serves as the regional office of the WHO, and the ReLAVRA. Table 3.6 shows the microorganisms subject to AMR surveillance in 2014 reported by nine countries in South America, each represented by an NRL.

During the analysis, particular attention was given to the eight priority pathogens identified by the GLASS network, which are also listed in the ReLAVRA platform. The selection of countries for this study was based on their proximity to the timeframe of the research and availability of AMR data supplied by them. Although the ReLAVRA platform offers data on AMR surveillance from 2000 to 2014, table 3.6 specifically focuses on the data from 2014. The countries, namely Argentina, Bolivia, Brazil, Chile, Colombia, Paraguay, Peru, Uruguay, and Venezuela, have reported AMR

Table 3.6. Total selected pathogens showing antimicrobial resistance in 2014 reported by nine countries in South America

Public health threat: 2014 South America AMR Surveillance of Infectious Agents									
Country	*Acinetobacter*	*E. coli*	*Klebsiella*	*N. gonorrhoeae*	*Salmonella*	*Shigella*	*S. aureus*	*S. pneumonia*	Total Isolates Reported
Argentina									
No. of Isolates Reported	1,649	**32,101**	1,56	679	646	2,778	9,549	410	49,372
Total % of AMR Isolates Reported	2.77%	53.97%	2.62%	1.14%	1.09%	4.67%	16.05%	0.69%	
Bolivia (Plurinational State of)									
No. of Isolates Reported	374	**6,245**	559	5	32	85	2,15	16	9,466
Total % of AMR Isolates Reported	3.48%	58.08%	5.20%	0.05%	0.30%	0.79%	19.99%	0.15%	
Brazil									
Number of Isolates Reported	1,296	808	611	X	**5,666**	49	3,422	26	11,878
Total % of AMR Isolates Reported	8.83%	5.50%	4.16%	X	38.59%	0.33%	23.30%	0.18%	
Chile									
Number of Isolates Reported	X	X	X	**1,184**	123	61	X	661	2,029
Total % of AMR Isolates Reported	X	X	X	46.09%	4.79%	2.37%	X	26%	
Colombia									
Number of Isolates Reported	1,594	**22,059**	11,513	83	1,099	323	17,273	433	54,377
Total % of AMR Isolates Reported	2.16%	29.96%	15.63%	0.11%	1.49%	0.44%	23%	0.59%	

Table 3.6. (*continued*)

Country	*Acinetobacter*	*E. coli*	*Klebsiella*	*N. gonorrhoeae*	*Salmonella*	*Shigella*	*S. aureus*	*S. pneumonia*	Total Isolates Reported
Paraguay									
Number of Isolates Reported	788	1,906	985	39	62	176	**1,989**	59	6,004
Total % of AMR Isolates Reported	9.54%	23.08%	11.93%	0.47%	0.75%	2.13%	24.08%	0.71%	
Peru									
Number of Isolates Reported	175	X	498	32	101	121	**1,071**	X	1,998
Total % of AMR Isolates Reported	6.50%	X	18.49%	1.19%	3.75%	4.49%	39.77%	X	
Uruguay									
Number of Isolates Reported	X	X	X	X	**220**	28	X	188	436
Total % of AMR Isolates Reported	X	X	X	X	43.65%	5.56%	X	37.30%	
Venezuela (Bolivarian Republic of)									
Number of Isolates Reported	183	**7,031**	1,058	X	198	242	3,412	180	12,304
Total % of AMR Isolates Reported	1.23%	47.19%	7.10%	X	1.33%	1.62%	22.90%	1.21%	

Source: Data aggregates reported by ReLAVRA 2014.

data for selected nosocomial, foodborne, and community-acquired pathogens. Out of the nine countries that reported AMR data on ReLAVRA, three countries enrolled in the GLASS network: Argentina, Brazil, and Peru. The study shows that Argentina reported a total of 49,372 isolates. The highest reported pathogen was *E. coli*, which accounted for 50%

of the total of 32,101 reporting that pathogen. Brazil reported a total of 11,878 comprising the eight pathogens. The most common pathogen reported by Brazil in 2014 was *Salmonella* spp., which accounted for 39% of the total of 5,666 reports for that pathogen. Lastly, Peru showed a combined total of 1,998 isolates and reported *S. aureus* as the most frequent pathogen (40% of 1,071).

The study revealed that during the 2018 GLASS data call, the GLASS report indicated that the United States had 5,061 patients who tested positive for *N. gonorrhoeae* (World Health Organization 2018a). In the 2019 GLASS data call, more information was added as the top pathogens posing a risk to the United States, as reported in an AMR data submission to GLASS, which were as *Salmonella*, *Shigella*, and *N. gonorrhoeae* (World Health Organization 2020g). Likewise, out of the eight bacterial pathogens, the most urgent threats in the United States in 2019, indicated by the CDC, included carbapenem-resistant *Acinetobacter* and drug-resistant *N. gonorrhoeae* (CDC 2019a). The pathogens that posed the most serious threats to the United States in 2019 included *Salmonella*, *Shigella*, *S. aureus*, and *S. pneumoniae* (CDC 2019a). Thus, awareness of and collaboration on AMR grew as surveillance of AMR and monitoring of pathogens increased.

Additionally, analysis is provided from a distinct perspective that focuses on a country–Ecuador–which is currently not enrolled in the GLASS network but follows the One Health approach as a member-state of the WHO (World Health Organization 2015d). The One Health approach involves the collaboration of various actors and sectors to address and mitigate global threats to public health in a comprehensive manner. By examining this country's AMR situation and surveillance efforts within the context of the One Health framework, a broader understanding of the interconnectedness between human, animal, and environmental health can be attained. Table 3.7 illustrates the country-specific AMR surveillance of Ecuador. As of the first GLASS data call in 2017, Ecuador had yet to submit AMR data in the GLASS network. Nevertheless, the Ecuadorian ministry of health and complementary private-actor networks continued to monitor and submit AMR data through WHONET to integrate bacterial AMR isolate-level data and facilitate data collection (Ministerio de Salud Pública del Ecuador 2019b).

Table 3.7. Infectious agents from Ecuador showing antimicrobial resistance most reported in WHONET

Resistance %	< 2014	2015	2016	2017	2018	2019	2020	> 2021
E. coli	58	64	63	61	X	X	X	X
Klebsiella	20	18	17	21	X	X	X	X
S. aureus	12	11	12	10	X	X	X	X

X = none reported.
Source: Ministerio de Salud Pública del Ecuador 2019b (Ecuador Ministry of Public Health).

Table 3.7 lists the microorganisms that posed a threat to public health in Ecuador as revealed during AMR surveillance conducted by the Ecuadorian ministry of health. These pathogens accounted for the highest proportion of isolates reported from 2014 to 2021. Furthermore, the study shows that Ecuador reported, from hospital services registered by the INSPI, *E. coli* as the most frequent (more than 60%) pathogen, followed by *Klebsiella* and *S. aureus* (Ministerio de Salud Pública del Ecuador 2019b).

The surveillance does not stop with GLASS but is carried out through other networks interconnected with GLASS. Therefore, the WHO Regional Office for the Americas and PAHO (AMRO/PAHO) encouraged ReLAVRA countries to participate in GLASS and capture additional variables to align with the GLASS methodology (World Health Organization 2018a). Thus, the GLASS and ReLAVRA interconnected networks included voluntary participation by countries and were deemed a form of control and monitoring of infectious diseases in a global system of AMR surveillance.

Managing Data Security: Controls for Regulatory Compliance

Are there regulations or process systems (security governance) that introduce new controls and protection in the GLASS network for the surveillance of infectious diseases? How does the rule relate to the GLASS provisions? From 2015 to 2019, the first GLASS phase was the early implementation stage of the GLASS process of AMR surveillance. The objective of GLASS is to "combine data on the status of enrolled countries' AMR surveillance systems with AMR data for selected bacteria that cause infections in humans" (World Health Organization 2017b, V). Moreover, GLASS aims to "launch the global surveillance system and provide guidance and technical support to countries on how to develop an effective national AMR surveillance system" (World Health Organization 2021d, 3). Under compliance metrics, the study tracks the number of controls for regulatory requirements. For example, security includes how actors handle and control data. The compliance metrics are the foundational precursor to discussing the five key dimensions of security governance discussed in the following case study section and to safekeeping laws or regulations in chapter 4. For instance, the investigation analyzes publicly available documents including government reports such as the those of the ministries of health of nation-states, which create security measures or protocols for safekeeping the information exchange ecosystem and controlling the spread of diseases.

Table 3.8. WHO-GLASS network data controls and compliance

Compliance metrics					
GLASS data call	**Date**	**Number of countries enrolled in GLASS**	**Source**	**Number of countries reporting AMR data**	**Source**
None	May 2021	109	(World Health Organization 2021d, iv, 3)	107	(World Health Organization 2021d, ix)
	Apr 2021	107			
4th Data Call	Aug 2020	94	(World Health Organization 2021d, 13)	70	(World Health Organization 2021d, 19)
3rd Data Call	Jul 2019	82	(World Health Organization 2020g, 7)	66	(World Health Organization 2021d, 19)
2nd Data Call	Dec 2018	71	(World Health Organization 2018a, 3)	49	(World Health Organization 2021d, 19)
1st Data Call	Dec 2017	50	(World Health Organization 2017b, 8)	22	(World Health Organization 2021d, 19)
	End of first data call	42			
Early Implementation Phase	2015-2019	GLASS objective: To combine enrolled countries' AMR data and surveillance systems for eight selected human bacterial pathogens			

Source: GLASS reports, World Health Organization (2016-2021).

In compliance with the IHR to prevent, protect, and control international spread of diseases (World Health Organization 2016a), GLASS fosters surveillance of AMR and global antimicrobial consumption. Table 3.8 illustrates the GLASS data calls created during the scope of the investigation. Between 2015 to 2021, GLASS placed four data calls. During each data call, participating member-states either enrolled or submitted AMR data to comply with the GLASS submission requirements and agreed to adhere to the IHR. Therefore, the WHO-GLASS network created aspects of controlling data by providing "sustainable control strategies to tackle the AMR threat" (World Health Organization 2020g, 118) and organizing the data from member-states to compile GLASS reports based on the data.

Managing Technology and Safety:
Risk Management Controls for Security Data Assurance

As part of the technological metrics analysis, institutional reports from 2015 to 2021 within the WHO-GLASS network were reviewed. This review sought to analyze risk management controls, specifically focusing on tracking the number of reports submitted by member-states to ensure security. By examining these institutional reports, insights can be gained into the effectiveness of the data-reporting processes and the measures in place to manage risks within the GLASS network. While using advanced technology, significant concerns include maintaining a database of client (customer) information and ensuring data security and integrity, credibility, and privacy. The network of GLASS contains a support detection component called the Emerging Antimicrobial Resistance Reporting (GLASS-EAR) (World Health Organization 2018a). The GLASS-EAR supports three features of AMR surveillance programs, namely, detection, early warning, and risk assessment, and provides tools for transparent and secure reporting. In searching for indicators of security assurances provided to countries in the submission and exchange of AMR data within the WHO-GLASS reports and results, attention was given to the presence of specific keywords. These keywords include [1] security, [2] safety, [3] privacy, and [4] data quality assurance. By examining the reports and results of the search for these keywords, it is possible to assess the extent to which security assurances are addressed and emphasized in the context of AMR data sharing and exchange.

The technological metrics in table 3.9 were developed as a baseline reference guide, providing an in-depth examination of data security and technical control mechanisms in the implementation of a surveillance system. The WHO-GLASS website and GLASS documents were reviewed to identify instances of data security assurance based on publicly available information. This approach offers insights into the measures taken to ensure data security and privacy within the surveillance system. The research shows that the term used most often concerning security was *quality assurance*. The reports mentioned little about data exchange security, safety, and privacy. However, data from the GLASS 2017-2018 report indicated that the WHO provides a comprehensive and formal policy to manage all databases and information sources securely (World Health Organization 2018a). Therefore, the technological metrics allow the study to encompass various aspects of security.

Table 3.9. Baseline reference technological metrics: security data assurance controls

AMR surveillance network and AMR data reports	Component	Security assurance*	Number of times the topic words were mentioned in relation to data and information exchange			
			Security	Quality assurance	Safety	Privacy
GLASS Report 2021	AMR	4	0	8	0	0
GLASS Report 2020	Early Implementation	4	0	4	0	0
GLASS Report 2017-2018	GLASS-EAR	1.4	3	5	0	0
GLASS Report 2016-2017	Early Implementation	4	0	6	0	0
2014 WHO Global Report on Surveillance	AMR	4	0	4	0	0
WHONET Manual	GLASS	1	1	0	0	0
2016 National AMR Surveillance System and Participation in GLASS	GLASS	4	0	4	0	0

* Code analysis: Investigating security assurances in AMR surveillance network and AMR data reports using the following keywords and codes: [1] Security, [2] Safety, [3] Privacy, [4] Data Quality Assurance.

Moreover, the GLASS-EAR reactivates information sharing through the WHO's data security policy which includes "information security, technical and physical data security" (World Health Organization 2018a, 232). Likewise, GLASS requires data quality assurance and removal of duplicate records from the data so that one isolate represents one patient to minimize the bias associated with reporting repeats (World Health Organization 2018a). In addition, during a high-level technical meeting in preparation for implementation of the global surveillance system, the conference assured participating member-states by noting that the "WHO had strict rules on reporting national data and very strict rules on data security" (World Health Organization 2017e, 13). Likewise, the WHO guided the confirmation of reports, the use of the IT platform, and adherence to best practices based on performance metrics (World Health Organization 2017e). For instance, the GLASS IT platform terms of use indicate that "access to the Web-based internet GLASS platform requires an electronic identification which consists of username, password and potentially other security measures" (World Health Organization 2015a, 2).

The terms also indicate that "all reasonable precautions have been taken to verify the content provided by the users into the Web-based internet GLASS platform" (World Health Organization 2015a, 2). Lastly, GLASS incorporated additional security checks and balances by checking the validity of the data through a "series of automatic checks built into GLASS" (World Health Organization 2017b, 17). Therefore, technology controls provide assurance and guarantees that data are protected from corruption or unauthorized access.

Furthermore, an essential point for clinical analysts to consider from an antimicrobial stewardship perspective is the necessity of having senior doctors sitting on the workbench. Having multiple reviewers conduct quality assurance to check the validity or security, for instance, a minimum inhibitory concentration (MIC) or the lowest concentration of a bacteriostatic agent, ensures that correct data and analysis are entered into the surveillance system. Also, according to the WHO, "countries are responsible for ensuring the validity, consistency, and completeness of AMR data submitted to

GLASS" (World Health Organization 2018a, 249). In addition, communication between actors, such as senior officials and clinicians, in analyzing the data is the key to ensuring the accuracy of information; labeling it as either sensitive, resistant, or intermediate; and determining whether the resistance is an actual threat. In other words, is the virus coming from inside the patient, or does the problem lie in sample collection?

Likewise, as clinicians obtain and enter relevant data contributing to a global surveillance network such as GLASS, they need to ask themselves: Is the bacterium triggering an infection? Thus, communication between senior doctors and colleagues ensures the validity of openly shared data. In turn, the results of the collective data provide transparency for the recipients of information. Therefore, a pre-analytic diagnostic check adds value to the overall global surveillance system of security governance in controlling the data and diseases during information exchange.

Dimensions of Security Governance

The five indicators of security governance are heterarchy, interaction of multiple public and private actors (depending on the issue), institutionalization, relations between actors ideational in character structured by regulations or norms, and a collective purpose. Security governance episodes from 2015 to 2021 are measured against the five leading indicators within the context of the WHO's GLASS for AMR. This assessment takes into account COVID-19 as a contemporary frame of reference, enabling a comprehensive analysis of security governance practices within GLASS during the specified timeframe. The key to understanding governance lies in analyzing which actors, other than the government, contribute to a "modicum of order, of routinized arrangements [that nourishes] the conduct of global life," since arrangements encompass complex forms (Rosenau 1992, 7; Brousseau, Marzouki, and Méadel 2012). For example, one mechanism of governance includes a top-down state intervention approach. However, "states, as well as markets, can fail" (Jessop 2000, 13). Moreover, adapting to continual innovations is valuable to security governance rather than hindering advancements (National Academies of Sciences Engineering and Medicine 2015). Therefore, the framework addresses the features of security governance in actor relations.

The concept of security governance involves multiple actors that conceive a system of rules in response to security threats. The set of processes guides international surveillance and structures collaboration. Governance includes acknowledging the importance of ideas, institutions, structures, and purposefully motivated actors (Webber et al. 2004). Dr. Nancy Campbell, Professor and Head of the Department of Science and Technology Studies, Rensselaer Polytechnic Institute, connected the concept of security governance of infectious diseases with being global. Further, actors often keep information generated through securitization too restrictive, and this type of information is shared as "open access, rather than corporate and proprietary" (interview, November 12, 2019). This section incorporates perspectives of security governance through document review and observations of actors from the northern and southern subcontinents of the Americas to analyze the emergence of a health regime on the surveillance of communicable diseases. Through the specific case study, the following sections address the five dimensions of security governance. In addition, the sections discuss the alignment between controlling the spread of infectious diseases and sharing data in the context of the emergence of a health regime.

Heterarchy: The Existence of Multiple Centers of Power

Global problems such as infectious diseases, cybersecurity, and possible disruptions from emerging technologies cross boundaries and involve coordinated actions taken by actors through multiple centers of power, or heterarchy. The first indicator of security governance is heterarchy, which involves relations of interdependence and includes a multiplicity of coordinated and combined actions that respond to the complex challenges of conducting affairs by actors such as the people, the state, or institutions (Webber et al. 2004). Similarly, heterarchy ensues as networks of interdependent social relations, which range from simple interactions between two actors to complex social divisions of activities (Jessop 2000). For example, the process of regulation or institutions that guide international surveillance involve diverse actors affected by the threat and potential sanctions by regimes to ensure compliance. The case study shows that the WHO's core responsibilities include "the management of the global regime for the control of the international spread of disease" (World Health Organization 2016a, 1). A plurality of actors or the existence of multiple centers of power stirs a movement of thought on inclusiveness, which constructs "decisions through the accommodation of interests" (Webber et al. 2004, 20). Therefore, sanctions, delivery, and accommodations construct ideas and decision-making by including many actors.

Some scholars of diverse perspectives tend to boost the role of the government, noting that states remain the agents which institute, finance, and realize governance structures (Peters 2007) or act as primary actors in global affairs (Grieco 1988). Furthermore, others see the states as strong and dominant units through a military and political lens (Buzan and Little 2000), and non-state actors as lacking a voice (Chorev 2012). However, a societal and economic perspective considers the states to be less prominent (Buzan and Little 2000). Thus, whereas some scholars err on the side of the state as a primary player, governance is necessarily state-centric.

Governance involves formal institutions and informal arrangements that actors agree to be in their best interest and also refers to any form of heterarchy of interdependent social relations, which range from simple dyadic interactions to complex social divisions of labor (Jessop 2000). In the area of security, traditionally reserved for the state, non-state actors play an essential role in monitoring and implementing security policies (Webber et al. 2004). In the area of security governance, both international organizations and states "remain the primary actors" (Webber et al. 2004, 6). Thus, states and international organizations play important roles in the international system.

The present study unveiled diverse contexts regarding the contribution of GLASS and the collaborative efforts among centers of power in AMR surveillance of infectious diseases, highlighting the emergence of policy issues. For example, a confidential interviewee said, "a rise of authoritarian autocratic regimes and a democratic regime which has strong protection of civil rights and liberties" (confidential interview with a professor at the

Rensselaer Polytechnic Institute, United States, November 9, 2019). On the other hand, a hardhanded information regime leans toward authoritarianism, insisting on solid state-controlled capitalism.

Confidential source. When you have a system that is good at identifying individuals and communities using high-tech means, you can't assume that these tools will be used in accordance with the United Nations declaration of human rights or the fundamental principles of liberal democracy (interview, United States, November 9, 2019).

However, the study centers on other forms of policy issues, such as a health regime involving multiple states that collaborate with a strong sense of responsibility and a focus on global health, civil rights, human rights, and liberties. As a result, each regime type exhibits varying degrees of heterarchy, blending multiple power players who are interconnected by a shared interest.

The case study shows that the WHA represents WHO's highest policymaking body and requested the WHO to establish GLASS through resolution WHA68.7 (World Health Organization 2015b). The WHO devotes energy to formalizing relations with nation-states. Collaboration works through multiple channels. For instance, the WHO collaborates "bilaterally, through regional networks and the WHO's regional offices, and through intergovernmental organizations and international bodies" (World Health Organization 2017b, 30). The WHO-GLASS brings new power centers to the surveillance network. According to available data, the WHO has approximately 30 collaborative centers, which work within the broad field of surveillance and resistance, laboratory capacity building, and external quality assurance. The collaborating centers form a network that provides expert technical advice to the WHO. The WHO creates protocols based on technical advice from collaborative centers. In addition, the WHO receives technical advice from various actors, including the Food and Agricultural Organization (FAO), the World Organization for Animal Health, the CDC, the European Centre for Disease Prevention and Control (ECDC), and the ministries of health. The WHA, which governs the WHO and comprises ministries of health worldwide, gives broad directions to the WHO. In turn, the WHO creates the plan, the WHA reviews the plan, and then the WHO's ministries of health agree on the plan's implementation. Likewise, through the GLASS technology system of AMR surveillance, the WHO adds to the security governance process by creating solutions where the member-states or expert collaborative centers provide input based on the data submitted. Therefore, these diverse high-level power centers collaborate towards a common goal.

The actor network theory assists in identifying the limitations of a network. If multiple actors with a common interest come on board and collaborate to respond to a threat, such interconnection in security governance of data and infectious diseases also "involves the incorporation of potential rivals" (Webber et al. 2004, 20). The study shows that 42 members enrolled in GLASS during the 2017 preliminary stage data call; 51, by January 2018; and 71, by December 2018, including Russia, but China did not provide information on the surveillance system (World Health Organization 2021d, 2018a, 2017b). As of April 2020, 94 countries had enrolled, but China remained unenrolled in GLASS (World Health Organization 2020g). One interviewee argued that China did not enroll owing to technical issues: the decision not to enroll was not politically driven (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Regardless, the study illustrates how participating and rival actors with the potential to collaborate in the surveillance network jointly manage common security matters. Russia, one of the great powerhouses in the international system, enrolled in the system. China, another power player, did not, but by 2020 its large size made it difficult for China to provide information from a system that provides aggregated data (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020).

Similarly, another of the great powers, the United States, considered AMR a national priority and took steps to fight the threat. For example, in 2014, the U.S. government established the U.S. National Strategy for Combating Antibiotic-Resistant Bacteria (CARB) (The White House 2014); in 2015, the U.S. National Action Plan for Combating Antibiotic-Resistant Bacteria (The White House 2015); and in 2020, the Second

National Action Plan for CARB (ASPE 2020). The national action plan for combating AMR also sets targets for the actions of different government agencies to address the global issue, providing an example of common rules to follow and a set of principles that make up a health regime. Likewise, the U.S. government engaged in multilateral organizational support through the CDC and the United States Agency for International Development (USAID) to support the sharing of data on antibiotic-resistant pathogens with the collaborating centers of other WHO member-states, including members of the GLASS network (ASPE 2020). In addition, the CDC collaborated with experts and world leaders to implement the national action plan. An interviewee remarked that the CDC used "several data sources and systems to track antibiotic resistance," (email interview with a person from the CDC staff, United States, February 17, 2020) including GLASS, to assess the scope of the problem and monitor AMR. Therefore, institutions such as the CDC look to AMR data from the WHO's GLASS as a reinforcement mechanism or to review the scale of the problem.

Likewise, as the world becomes more complex, and as social and economic conditions emerge that nation-states or the market cannot manage, reliance on networks and heterarchy increases. The WHO supports the member-states in strengthening infection control measures, preparedness, and responses to outbreaks of infectious diseases, and GLASS supports and fosters global and national AMR surveillance (World Health Organization 2021d). Digital transformation across all aspects of life and maintaining coherence are also significant. Institutions such as the WHO act as a bridge between actors to ensure inclusivity among nation-states, keep the different processes together, warrant universal principles over time, ensure that information is shared, and engage in capacity building. The real value emerges when institutions and a health regime facilitate the pulling of actors together, including sovereign entities. As we peel back the onion, the liberal institutionalism theory notes that the states maintain a primary role. However, the institutions themselves, particularly a health regime that includes a global AMR surveillance structure, are built by actors who aspire to have a supranational governance structure, such as the UN, and undertake regional efforts toward common goals. One example of this in which various member-states enrolled and participated is the GLASS network. This health regime works because of multiple centers of power. The institutions, therefore, are just as significant actors in the international system as states. Thus, a more robust and substantial commitment to collaboration, enhancing digital literacy, and clarity on data distribution and results help solve various challenges from AMR to a pandemic and the digital sphere.

Interaction of Public and Private Actors

The second indicator of security governance involves interaction between public and private actors working together. The multiplication of actors involved at various levels adds to security management while diffusing a global health crisis. Moreover, each actor brings a different set of potential "incentives to the resolution of the crisis" (Webber et al. 2004, 11). Getting the perspectives of other customers, such as officials or citizens, is critical because diverse voices are essential at the table. Thus, a minimal working relationship between public officials and private actors creates a positive engagement in crisis management.

In addition to institutional multiplication, "the process of delivering security involves many actors whose inputs were previously negligible or non-existent" (Webber et al. 2004, 16). Tackling a global issue involves reassembling and collating resources from non-governmental and private actors. Such diverse actors include economic investors, judges, construction companies, police officers, medical professionals, staff of charities, and administrators (Webber et al. 2004). The network analysis conducted earlier identified the diverse actors in the network and their interconnectedness. This research considered multiple types of actors that connected directly to the primary unit of analysis and other relevant actors with as much common interest in the boundary object.

The case study shows private interest groups such as philanthropic organizations that participate in the collaboration and interconnectedness for information sharing as envisaged by GLASS and use the software, WHONET, that manages data that countries use to prepare the information submitted to GLASS. For example, private actors interconnected with GLASS and the WHONET include the Bill and Melinda Gates Foundation and, as one interviewee remarked, "in the area of tuberculosis, the IUTLD or the International Union Against Tuberculosis and Lung Disease, and Doctors without Borders" (interview with Dr. John Stelling, January 24, 2020). Likewise, the Pew Charitable Trusts (PEW), an NGO, focused on domestic policies but looked to connections and information from sources such as the WHO's GLASS data and network to maintain and raise awareness of global efforts.

PEW executive. On its face, having increased additional information on what kinds of resistance are being seen at the country level, worldwide, and being able to use that data to look at patterns and to identify areas where additional work is needed, is helpful and useful, and you've seen that in other communicable disease spaces. So, surveillance is definitely an essential aspect of any sort of global effort to address the spread of resistant pathogens (confidential interview, United States, January 29, 2020).

In addition, PEW and the WHO have worked closely on a pipeline in the creation of antibiotics and demonstrate what drugs are showcased in the FDA development process. The Pew Charitable Trusts set up the pipeline and criteria; the WHO communicated with PEW to understand the process; and subsequently the WHO created its own pipeline to expand globally, using the information PEW had shared (confidential telephone interview with an executive at the PEW Charitable Trusts, United States, January 29, 2020). Therefore, the example is of collaboration between a private actor (PEW) and the WHO, which worked together to highlight the challenge and problem of a limited pipeline. Similarly, in 2020, the Global Antibiotic Research and Development Partnership (GARDP) participated in a session organized by the HHS on combating AMR The basis of GARDP, an independent foundation founded by the WHO, is nonprofit collaborative approaches. The partnership conducted R&D and clinical development of AMR treatment based on the collection of surveillance data from the WHO-GLASS program (Piddock et al. 2022) and also provides a delivery path for innovations developed by private and public sectors in the United States (U.S. Department of Health & Human Services 2020b). The WHA gives observer status to these private actors, which present statements, advice, guidance, and funding. At times, philanthropic entities, governments, and international bodies have backed the sheer drive by institutions to ensure that funding gaps close as quickly as possible, the regulatory environment works as efficiently as possible, and global markets and supply chains are ready whenever required.

The case study further shows that the number of member-state enrollments had increased to 109 countries and territories by May 2021 in the GLASS network (World Health Organization 2021d). In addition, the study reveals that Brazil, Argentina, and Peru enrolled in GLASS from among the countries of the southern subcontinent of the Americas between 2015 and 2021. Ecuador used WHONET but was unenrolled in GLASS by the end of 2021. The National Institute for Public Health Research of Ecuador noted that until 2010 there were 22 public and private hospital laboratories coordinated by the private Hospital Vozandes in Quito to monitor bacterial resistance worldwide (INSPI 2021). The INSPI is the national reference laboratory of the Ecuadorian ministry of health (INSPI 2021). In addition, the INSPI interconnects with other institutions such as the U.S. CDC. For example, owing to the COVID-19 pandemic, the CDC sent diagnostic materials such as primers and positive controls to reference laboratories, including the INSPI in Ecuador, rather than to private laboratories, for testing. Therefore, the connection between ministries of health is through their respective national reference centers.

The growing awareness of the threat that AMR poses to public health motivated the first meeting, held in 1998 in Caraballeda, Venezuela, organized by the PAHO and the Pan American Association for Infectious Diseases with support from the Venezuelan ministry of health (Salvatierra-González and Guzmán-Blanco 1999). As a result, the union of Latin American countries was formed for the first time to organize surveillance on AMR (Salvatierra-González and Guzmán-Blanco 1999). The conference recommended that the public-sector actors oversee the management of the networks. Each country began monitoring AMR through its respective national reference centers. For this case study, an interview was conducted with a medical doctor and microbiologist, who was among the attendees at the conference. The doctor created a small network with five friends from different laboratories because they had to be vigilant on AMR since Ecuador lacked knowledge about the resistance of bacterial pathogens such as *Shigella* to antimicrobials. The interviewee, an Ecuadorian medical doctor and microbiologist and temporary advisor of antimicrobial resistance at the PAHO, who worked in the private sector, was invited to the Caraballeda meeting by PAHO, a regional organization that knew about the small Ecuadorian AMR network group. During the meeting, the members committed to monitoring resistance and sending the data to PAHO. As a result, the interviewee created the Red Nacional de Vigilancia de Resistencia Bacteriana del Ecuador (National Bacterial Resistance Surveillance Network of Ecuador, REDNARBEC for its initials in Spanish) to monitor AMR in the country and to contribute as a member of the WHO network to the surveillance of bacterial resistance worldwide (INSPI 2021). The REDNARBEC began with ten laboratories sending data to PAHO. By 2010, under the coordination of Hospital Vozandes and the interviewee, REDNARBEC had grown to 22 public and private hospital research centers (INSPI 2021).

When asked for the reason for the abrupt stop to sharing the data on Ecuadorian AMR surveillance since 2010, the interviewee, who was working at the time in the private sector, at Hospital Vozandes, indicated that the hospital was initially a reference center that received data from peripheral laboratories. The doctor explained: “I analyzed the data, cleaned the data, and all the information that was published up to 2010 was sent to the Pan American Health Organization” (confidential telephone interview with an Ecuadorian medical doctor, microbiologist, and temporary advisor on antimicrobial resistance at the PAHO, by telephone, Quito, Ecuador, February 25, 2022). The doctor noted that when the Correa government (2007-2017) came to power, it nationalized everything, and wondered how a private laboratory held the data for a global surveillance network (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Nevertheless, for the WHO, “the involvement of private hospitals is crucial to generate more representative AMR surveillance data" (World Health Organization 2021d, 19). Likewise, during the second high-level technical meeting on AMR surveillance for local and global action to facilitate data sharing by national bodies and stakeholders, countries in the Americas region indicated that the private sector and academics report to the national authority, which then reports to the WHO (World Health Organization 2017e). Thus, the Ecuadorian private hospital collaborated to exchange information related to pathogens and network structure with the Ministry of Public Health. After training the new government personnel on how to enter and extract the data from the REDNARBEC, the interviewee claimed that "REDNARBEC disappeared, everything went to the government, and AMR surveillance went to INSPI in 2011" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Therefore, a private-sector actor (Hospital Vozandes) collaborated in sharing data with a public-sector actor (INSPI) in the surveillance of bacterial pathogens.

The gap, which lasted longer than ten years, between the last data submitted to PAHO by the Ecuadorian AMR network and the present creates data discrepancies. The interviewee noted that the problem with data with such gaps is that "you have to make use of that health data so that they have an impact and make public policies" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Furthermore, "they have to be super clean, well-filled data, because the one who types can input wrong information, make mistakes, and get things that are not correct" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Therefore, the lack of updated or published information on resistance provided by the country poses significant issues.

Many factors contributed to the failure to post timely sequential data. For instance, the interviewee believed the information was missing because "the administration does not have the money or enough personnel, we are not blaming the public sector, but it is challenging-everything is a lack of public policies" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Nevertheless, a blanket of political corruption covered the Ecuadorian public health system. The doctor added that they placed officials who are not experts in epidemiology or AMR, and "they place officials because he is a friend of the cousin who voted for the president or vice-president, totally corrupt" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022).

Under the 68th World Health Assembly Global Action plan on AMR (2015), member-states, including Ecuador, committed to developing their national action plan to adhere to the objectives of the *One Health* approach, including tackling AMR (World Health Organization 2015d). Accordingly, the Ecuadorian ministry of health created its national plan for the prevention and control of AMR (Ministerio de Salud Pública del Ecuador 2019a). Furthermore, the Ministry of Public Health counts on monitoring AMR through the Sistema Integrado de Vigilancia Epidemiológica (Integrated Epidemiological Surveillance System, SIVE for its initials in Spanish), by notifications from the WHONET system (Ministerio de Salud Pública del Ecuador 2014). In addition, the microbiology laboratories of the hospitals of the Ministry of Public Health and of the Instituto Ecuatoriano de Seguridad Social (Ecuadorian Social Security Institute, IESS in Spanish), the Instituto de Seguridad Social de las Fuerzas Armadas (Social Security Institute of the Armed Forces, ISSFA in Spanish), Instituto de Seguridad Social de la Policia Nacional (Social Security Institute of the National Police, ISSPOL in Spanish), and a complementary private network work with the WHONET database (Ministerio de Salud Pública del Ecuador 2019a, 2019b). In turn, the INSPI developed the techniques to detect the pathogens that showed resistance and updated the WHONET, which manages and analyzes data from microbiology laboratories.

Unfortunately, the interviewee said that the last surveillance data came from the private-actor network REDNARBEC in 2011 (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). Nevertheless, the INSPI submitted old data (2021) to the 2014 AMR Global Report on Surveillance reported by the WHO. The data from Ecuador focused on surveillance for resistance in common bacterial pathogens. The report served as the basis for GLASS to integrate

AMR data (World Health Organization 2014). Furthermore, according to an official government document, Ecuador "still does not have data on the consumption of antibiotics and those used in infectious diseases in the field of human and animal health" (Ministerio de Salud Pública del Ecuador 2019a, 14). Thus, the lack of systematic tracking of AMR data leads to a gap in the case of some member-states in terms of enrollment, data submission, and exchange in GLASS, as in the case of Ecuador.

Implementing AMR surveillance means that actors must collaborate, influence, and work toward integrating the policy instruments with a number of other actors, perhaps even outside the WHO-AMR sphere. For example, a diverse set of public and private actors attended a virtual official meeting of the PACCARB on AMR and COVID-19 (U.S. Department of Health & Human Services 2020a). The meeting included the following actors: one designated federal official, two advisory council staff, eight organizational liaisons, eleven regular government employees, and fifteen voting members (U.S. Department of Health & Human Services 2020a). Therefore, the study reveals that a more significant interaction of intelligence sharing between diverse actors adds to collaborative interactions and exchange of ideas in response to the crisis on infectious diseases and AMR.

Furthermore, caution lies in striking a balance between the rights of the public sector regarding privacy and data protection and the private sector's need to leverage big data. On the one hand, actors such as the WHO and GLASS prioritize privacy while implementing AMR surveillance. We are dealing with a target in intelligence just as the WHO developed GLASS. The targeted entity in the surveillance network comprised eight bacterial pathogens of human significance that showed AMR. On the other hand, nation-states allow technology unicorns to be born. For instance, during the COVID-19 pandemic, telemedicine, digital meetings, and digital products increased. To disrupt the coronavirus's transmission chain, governments in the global South adopted new mobile applications: Argentina (Cuidar), Bolivia (Bolivia Segura), Brazil (Coronavirus SUS), Chile (CoronApp), Colombia (CoronApp), Ecuador (ASI Ecuador), Paraguay (COVID-19MX), Peru (PeruEnTusManos), and Uruguay (CoronavirusUy) (Pan American Health Organization 2021;

Gobernación de la Provincia de Loja 2020; MINTIC 2020; Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento 2020). Thus, closing the digital divide between the public and private sectors entails collaboration, transparency, and security reliability.

Similarly, the worldwide spread of infectious diseases brought forth the involvement of additional actors, such as intelligence and security officers, to deliver security and other networks. As a result, stakeholders introduced security-related elements, such as more think tanks focused on security issues during the COVID-19 pandemic. In addition, media attention regarding security measures increased from immediate transition into the digital space. Likewise, focusing on the subsequent silent tsunami of antibiotic-resistant infections opened the door to other actors, such as R&D centers, biotechnology companies, microbiologists, investors, and financial institutions, responding to the threats.

The sudden outbreak of the new virus and various actors' actions to combat the disease reinforced collaborative and interconnected global responses, which have been quicker and more transparent than those at the time of the 2002 SARS. Here we have these organizations in this complex system having to address a risky scenario. In 2019, once China informed the WHO of the nontraditional threat, the United States and other global countries began close surveillance. Various actors, including the ministries of health, the CDC, the military, and the health care community, banded together to combat the threat. In January 2020, the second meeting of the Emergency Committee by the WHO Director-General under the IHR took place in Geneva to determine a Public Health Emergency of International Concern (PHEIC). In February 2020, the WHO convened a global research and innovation forum in Geneva to mobilize international action in response to COVID-19, which brought together key actors from the ministries of health, research funders, scientists, and public health agencies. In March 2020, global policymakers held an emergency call where G7 leaders discussed economic response mechanisms tied to the outbreak. In April 2020, the G20 leaders held a virtual conference to discuss ways to combat the pandemic. Therefore, multiple public and private actors have become essential in preparedness and response to calamities and threats.

The pandemic experience demonstrated how essential connectivity was, and the marked digital divide. Private-sector actors working with governments and agencies have helped to promote economic development to close the digital divide. A sense of security is essential to generate assurance and significant steps. For instance, the NRLs acting as core components "secure the correct flow of information to national bodies and GLASS and are essential in data preparation and submission" (World Health Organization 2021g, 17). Likewise, the first GLASS data call in 2017, which attracted 40 countries and eventually more than a hundred countries, secured a strong commitment and close collaboration with AMR regional networks. This is a minor example and showcases important steps leading to dynamic changes.

Formal and Informal Institutionalization

The third indicator of security governance entails the employment of institutions, such as the observance of norms and frequency of actions and decisions (Holsti 1992, 50). Actors create a system of governance through agreement on the pertinence of institutions in carrying out governance tasks (Holsti 1992, 36). For retired Colonel Patrick J. Mahaney, Jr., U.S. Army, Officer of the Department of Defense, United States Special Forces (Green Beret), security governance includes "monitoring because you want to detect quickly whenever there is some sort of an outbreak and that is done by various means, such as taking temperatures" (interview, United States, February 14, 2020). Likewise, attention to institutions, transnational organizations, corporate interests, civil society, the state, and government characterizes governance perspectives (Pierre 2000). Nonetheless, the significance of security governance includes the gray area that results from developing informal and formal institutions-from participating countries to non-members in the core surveillance system. Therefore, the WHO has striven to form associations with diverse players.

The results in chapter 3 mapped four distinct networks, which included the most influential actors in the collaborative network. Mapping the networks helped to identify which relevant institutional actors were predominant in the collaborative network for surveillance of AMR. At an institutional level, to strengthen multisectoral actions to tackle AMR and deliver on the 2030 Agenda for Sustainable Development, during the 75th session of the UN General Assembly, the co-chairs of the Group of Friends on Tackling Antimicrobial Resistance launched the “Call to Action on AMR” (World Health Organization 2021b). As of December 2021, the Call of Action included 113 member-state signatories, including Argentina, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay, and Venezuela from the global South, and 39 supporting organizations, including those from the private sector and civil society (World Health Organization 2021b).

At a practical level, the WHO informally engages with each of the participating member-states through consultations in meetings and activities on common interests such as tackling infectious diseases and AMR. The case study shows that during the coronavirus pandemic, from November 28 to December 9, 2020, PAHO, in collaboration with WHO headquarters, held four online regional consultations (World Health Organization 2021d). The informal online sessions aligned with the framework of online consultations to prepare for the third high-level technical consultation and meeting on AMR surveillance and its use for concerted action (World Health Organization 2021d). More than a hundred diverse online participants attended each session, including “microbiologists, epidemiologists, clinicians, public health professionals from ministries of health and partner institutions” (World Health Organization 2021d, 59). The online actions of both PAHO, as the WHO's regional office for the Americas, and the WHO's headquarters, collectively illustrate the attainment of the strategic global action plan objective. This objective includes understanding and improving awareness of AMR, as well as “to provide support and technical assistance to countries, with a specific focus on low- and middle-income countries” (World Health Organization 2015d, 19). Furthermore, collaboration by participating attendees in providing feedback on the GLASS documents and system helped to ensure technical cooperation from countries. Therefore, the informal online meetings contributed to the development of continued strength of AMR surveillance in the Americas.

Moreover, the WHO assumed an important role in connecting with other institutional actors such as funders and NGOs. For instance, according to the WHO Situation Report 85, groups of funders, manufacturers, doctors, and scientists pledged to collaborate with the WHO to push for the accessibility of a vaccine for COVID-19 (World Health Organization 2020e, 2020u). As an institutional structure, the WHO has become a conduit for dialogs and consultations relating to global health, safety, and security and an informal and formal link to other actors, especially at the UN. Therefore, adding new institutional actors adds to the complex interdependent channels that connect societies.

According to one interviewee, "on the GLASS side, we are actually following the principles and rules of the WHO, which respond to the whole UN system" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Three critical aspects to consider during a continuum of engagement with nation-states and international organizations worldwide are a committed democracy, privacy, and respect for individuals. The WHO works with the member-states and the ministries of health (World Health Organization 2018b). According to a WHO official, the organization accepts data from member-states through official channels, and "the data coming to GLASS comes through official focal points appointed by the national branch of government, the ministry of health" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Lieutenant Colonel Arnel P. David explained, "if you don't have some kind of organization managing it, to manage people's participation, their curation of the data, then it's going to be an abused resource" (interview, February 10, 2020). Lieutenant Colonel David is affiliated with the United States Army, Strategic Analysis Branch. He is also a United States Special Assistant to the Chief of the General Staff and Deputy Assistant Chief of Staff (DACOS) G5 of the NATO Allied Rapid Reaction Corps. The case study reveals that under the WHO, GLASS "applies a set of rules to its data analysis to ensure reliability of generated results" (World Health Organization 2018a, 6).

Moreover, "surveillance National Focal Points (NFP) have been identified in all countries, working closely with the GLASS Secretariat alongside WHO regional offices, country offices, and regional networks"

(World Health Organization 2017b, 5). For instance, with regard to the enrollment of Brazil in the GLASS system, an official indicated, "we have a national focal point officially appointed by the Brazilian government and one of the national institutions responsible for the coordination of national surveillance system, so that is the formal regulation" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Likewise, GLASS "collaborates with existing regional and national AMR surveillance networks to produce timely and comprehensive data" (World Health Organization 2015b, 7). Furthermore, institutions such as the WHO have acted as a bridge or accelerator in some bottom-up approaches to ensure coherence by bringing different actors together.

In addition, the regional surveillance networks collect aggregated data provided by NRLs. For example, the GLASS report notes that in 1996 "the WHO Regional Office for the Americas Pan American Health Organization (AMRO/PAHO) established the Latin American Network for Antimicrobial Resistance Surveillance (ReLAVRA)" (World Health Organization 2017b, 124). Moreover, in the beginning, the ReLAVRA surveillance network was limited to reporting AMR data on foodborne pathogens. However, the network expanded to cover surveillance of the GLASS-selected pathogens for AMR (World Health Organization 2017b).

Likewise, an example of informal institutionalization is that between the AMRO/PAHO and the ReLAVRA participating countries in the ReLAVRA surveillance network. AMRO/PAHO ensured "continued communication within the network, bimonthly Webex meeting with ReLAVRA participants take place, joined by technical experts and partners" (World Health Organization 2017b, 124). Furthermore, the PAHO office worked with countries in the region and encouraged ReLAVRA participants to enroll in the GLASS network. Therefore, the connection and fostering of networks such as GLASS and ReLAVRA have expanded global monitoring of AMR to address global health threats.

Nonetheless, one interviewee presented areas of concern by noting that, on the one hand, intelligence testing through open data assisted in collecting information to address a problem. Nevertheless, on the other hand, actor mindfulness in reporting information during categorization is essential. The interviewee indicated that intelligence testing is used "to determine the abilities and characteristics of certain people and groups and we form public policies based upon wise spending of money" (confidential interview, United States, November 9, 2019). Although shared health data do not link the identities of individuals to the information per se, and reporting by the organization and the information presented are so structured as to prevent the data being connected to specific ethnic groups, so that you have a "supposedly neutral technique, which turns out not to be neutral" (confidential interview, United States, November 9, 2019). The study shows that GLASS aggregates statistics based on country and a limited number of antibiotics. For example, GLASS wants to know, according to Dr. John Stelling "the percent MRSA at the national level. So, there is nothing by region, nothing by facility. They would like it to be feasible by male, female, age group, and infection origin" (interview with Dr. John Stelling, United States, January 24, 2020). The interviewee added that the WHO "does not want to know the name of the hospital or the names of the patients," but rather the GLASS asks for high-level summaries of things often associated with surveillance for advocacy purposes (interview with Dr. John Stelling, United States, January 24, 2020). Focusing on "interdependence, divisions of knowledge, reflexive negotiation, and mutual learning" (Jessop 2000, 18) in the exchange of publicly available data on the surveillance of AMR to reduce the incidence of infectious diseases creates new network paradigm shifts toward partnerships and the informal sector. Thus, analysts and data scientists consider data gathering and judgments made about groups of people or countries during the intelligence testing process.

In various instances, institutions demonstrate their responsiveness to security threats through their actions and decisions. For instance, the WHO identified AMR as a significant global public health concern, ranking it among the top ten threats facing humanity (World Health Organization 2019b, 2020b, 2021i). The WHO emphasized that AMR poses a substantial risk to global health, food security, and development (World Health Organization 2020a). As a result, by 2019, the WHO officially recognized AMR as one of the foremost threats to global health, functioning as a securitizing agent. Similarly, in January 2020, the WHO declared COVID-19 a public health emergency of international concern, and the Secretary of HHS declared a public health emergency in response to COVID-19 (U.S. Department of Health & Human Services 2020c; Executive Office of the President 2020). In March 2020, the WHO characterized the virus as a pandemic (World Health Organization 2020w). As a securitizing agent, President Trump declared the COVID-19 outbreak in the United States a national emergency (Executive Office of the President 2020). In addition, the administration granted all 50 states, tribes, territories, and the District of Columbia emergency disaster declarations and protective measures in response to the coronavirus outbreak (FEMA 2020). Therefore, in both scenarios, the actions of the securitizing agents created the perception of a security threat by showing the world through its frequency of activities that it was facing multiple health challenges.

Ideas Between Key Actors Driving a Surveillance System

The assembling of information and ideas between actors evolves over time. As vast amounts of data overflow amass the information ecosystem coupled with technological advancements and global threats, time is essential in understanding the means to the end. The fourth indicator of security governance involves the relations between actors that are ideational in character and structured by understandings and norms. It pertains to comprehending the significance of actors' actions within the governance process of infectious diseases surveillance. This involves understanding the interactive ideas, their relevance to the network, and the relationship among actors in connection with the ideas and resulting actions. The ideational indicator encompasses a consensus between actors on governance tasks (Webber et al. 2004; Holsti 1992). Scholars in different disciplines study the role of ideas in public policy, introducing an ideational approach (Kisby 2007). Some stress the importance of ideas surrounding a network (Marsh and Smith 2000). In accordance with this approach, analyzing security governance needs to consider the role of ideas promoted by relevant network members. The ideational characteristic of governance by institutions protects, preserves, and promotes ideas through inscription devices such as legal instruments. Thus, part of the collaborative network on security governance builds on the ideational context through which relevant actors operate.

A proliferation of government initiatives is found worldwide, not only confined to the United States or the global South. Each nation-state develops its regulatory framework. For instance, the IHR brought together member-states for a common framework to inform AMR surveillance through the capacity to test for susceptibility to antimicrobials. The IHR stipulated "the requirement for access by States Parties to capacity for investigation of any disease outbreak that may represent an international public health threat" (World Health Organization 2014, XIX). Likewise, the WHO's GLASS brought together participating member-states to foster and strengthen AMR surveillance systems in each country to guarantee the knowledge and systemic production of reliable data. The case study revealed that the WHO developed GLASS, in accordance with the WHA resolution, "to support the implementation of the Global Action Plan on Antimicrobial Resistance adopted at the Sixty-eighth World Health Assembly in May 2015" (World Health Organization 2015a, 1; World Health Organization 2015d). The participating member-states favored the GLASS surveillance, including the relevant task of transmitting information onto the WHONET. On a more focused scale, the ideational characteristic includes enlargement (Webber et al. 2004). Enlargement develops into actions of actors that increase in nature. For instance, the ongoing development of new tools and capacity building included expert consultation, which took place in 2021, on the burdens of AMR. An expert network was established in 2021, which focused on the application of the surveys in countries. A new WHO academy was created to explain surveillance standards and data requirements; WHO is projected to reach 10 million global learners by 2023. Additionally, GLASS developed comprehensive training on AMR surveillance for policymakers and professionals in 2022 (World Health Organization 2021d).

Moreover, the instrument remains a boundary object when diverse actors collaborate independently and interpret GLASS differently to promote a health regime in the complex and interdependent power relations among actors. The actors create a system of "ideational consensus" (Holsti 1992, 36) based on ideas or norms which underpin governance (Webber et al. 2004), such as avoiding past issues of pandemic disasters and eradicating infectious diseases. One academic interviewee noted that "in regard to legislation and regulation, there ought to be open debate of relevant people with useful knowledge and then there ought to be debates from different points of view" (confidential interview, United States, November 9, 2019). This study reveals that on February 26-27, 2020, the HHS organized a session to hear experts discuss innovations to combat AMR (U.S. Department of Health & Human Services 2020b). Listed on the meeting summary were 64 invited participants, including public health institutions, experts from the academia, military, patient advocates, research institutions, media editors, pharmaceutical companies, and NGOs (U.S. Department of Health & Human Services 2020b, 36-38). The study revealed that a diverse group of actors came together to discuss their ideas on health innovations and the rapid spread of COVID-19, which illustrates civil society's vulnerability to emerging infectious diseases. Dr. Martin Blaser, PACCARB Chair, emphasized that "building the infrastructure for combating AMR will help address COVID-19 and other such threats" (U.S. Department of Health & Human Services 2020b, 1). The exchange of ideas in the meeting revolved around innovations to fight AMR, such as alternative therapies, new antibiotics, vaccines, diagnostics, and animal-health management products. For instance, the meeting expressed interest in novel technologies to reduce pathogens on surfaces. Participants suggested that the Bill and Melinda Gates Foundation invest in developing a vaccine for *Streptococcus* in the neonatal health initiative. A key representative of the foundation indicated that "the foundation has funded development of two vaccine candidates that are currently in preclinical and clinical trials" (U.S. Department of Health & Human Services 2020b, 11). Likewise, GARDP addressed its clinical R&D of treatments to treat drug-resistant infections in hospitalized adults, infants, and children. In addition, it focused on the CDC and the WHO's priority pathogens also researched in GLASS.

Furthermore, the meeting was intended to "gather information and exchange ideas about One Health issues and AMR" (U.S. Department of Health & Human Services 2020b, 1). The sharing of information by critical executives brought viewpoints that ensured that the updated national action plan, released by the HHS at the end of 2020, reflected the current state of AMR threats (ASPE 2020). Therefore, the ideas exchanged by diverse characters during the session reinforced the process that guides international surveillance of infectious diseases.

In considering security governance as a system of rules, the WHO, through the GLASS surveillance system, served as a conduit between actors to collaborate on the idea of surveilling infectious diseases. As one official indicated, "For us, the primary purpose of the GLASS, the system, is not the global data collection, it's supporting countries in building their national systems" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Another interviewee noted data ownership, access, and use of WHONET: "data belongs to the country and the WHO is the steward of the data, and manages the data with the permission of the country" (interview with Dr. John Stelling, United States, January 24, 2020). Thus, as an institution, the WHO acted as a communication channel and guided the international surveillance of AMR, supported by nation-states.

At the forefront of preparedness and response are efforts to address threats, including sharing ideas for knowledge production in network communities to tackle AMR, addressing the COVID-19 pandemic, and overcoming financial or regulatory barriers. Furthermore, an ideational interaction between customers or key officials generates alternative ideas. However, the challenge is security channels that keep progress and innovation from moving. For one interviewee, security governance entails consideration of the following issue:

Confidential source. If you wanted to have the medical service and even the medical testing, as the affected individual, you ought to be certainly informed. If the data with the ability to trace it back to that particular individual were part of the package, then you ought to have an oversight and right to a voice, including denial (interview, United States, November 9, 2019).

The case study shows that, in submitting AMR data, users of the web-based GLASS platform agreed that the "data submitted have been collected in accordance with applicable national laws, including data protection laws aimed at protecting the confidentiality of identifiable persons" (World Health Organization 2015a, 1). Moreover, the WHONET contains a feature that assists software users in setting up passive surveillance systems that pool and analyze users' files collaboratively (O'Brien and Stelling 1995). Likewise, the WHONET provides "file encryption options to ensure confidentiality before data are pooled and analyzed" (O'Brien and Stelling 1995, 66). Therefore, institutions and nation-states consider a critical aspect from the beginning of the data collection surveillance process, namely, how to build these applications so that procedures, such as de-identification, balance the results of data collection.

Likewise, the manual for early implementation of GLASS on the surveillance of AMR with respect to bacterial pathogens that infect humans reveals that the WHO provided reports during the WHA to member-states and ensured "respect for member-states' laws on surveillance, data collection, storage and reporting, and patient confidentiality" (World Health Organization 2015c, 15). Therefore, when distributing the WHO-GLASS manual to participating member-states, the enrollees are notified that private information and any information that enables identification of individuals will be protected when enrolling or submitting AMR data GLASS surveillance system.

For the United States, the state of global affairs in the last ten years "represents a particularly powerful and hegemonic vehicle for the projection of certain ideas of democracy, markets and institutional commitment" (Webber et al. 2004, 7). For example, in March 2020, Pfizer called on all members of the innovation ecosystem, including small and large biotech companies, government agencies, and academic institutions, to come together and address the global health crisis (Pfizer 2020b). As this example shows, the idea of safety, health security, and taking collaborative measures to combat a global threat has been at the forefront during health crises. On September 8, 2020, nine biopharmaceutical companies–AstraZeneca, BioNTech, GlaxoSmithKline, Johnson & Johnson, Merck, Moderna, Novavax, Pfizer, and Sanofi– pledged to work as a unit across the industry harnessing scientific expertise and technical skills to combat the crisis (Pfizer 2020a). Thus, these agents of continuity have striven to address safety and security concerns through collaborative efforts inspired by the idea of addressing present and future global threats to health.

At the other end of the spectrum, complications arise in pushing forward ideas or an agenda to stabilize health care issues such as AMR. For instance, in Ecuador, ideas seem to be transitory in the political sphere and liable to change as each new administration brings in new ideas. As the interviewee said, "You can have a law that is very good, but the Ecuadorian assembly does not approve it because they have no political interest" (confidential interview by telephone, Quito, Ecuador, February 25, 2022). Similarly, as officials and the ministry change positions in Ecuador, the information saved in the network disappears with the old administration. The new administration does not build upon what scientists have created. Instead, the interviewee added, "An official enters, and all of the prior research is wrong with no design policies" (confidential interview by telephone, Quito, Ecuador, February 25, 2022).

Nevertheless, in the past ten years, Ecuador improved its surveillance mechanisms such as monitoring AMR in animals. The idea of recognizing resistance as a significant health threat brings to the forefront the tracking of the use of colistin as an antibiotic medication in animals. Antibiotics such as colistin, quinolones, and fosfomycin are commonly used in poultry production in Ecuador (Ortega-Paredes et al. 2020). However, the WHO lists these antibiotics as critically important antimicrobials for human medicine (World Health Organization 2017a). In 2019, the Ecuadorian administration banned colistin in poultry meat (Ortega-Paredes et al. 2020). For Ecuador, "the most important source of animal protein with a per capita consumption of poultry meat of 30.4 kg/year" is its poultry products (Ortega-Paredes et al. 2020, 2). However, who indeed checks that these antibiotics are not used by citizens? For instance, if a farmer owns 40,000 chickens that are going to die because of an outbreak of infectious disease, the farmer will use colistin and may not care about resistance: the farmer wants to save the 40,000 chickens and, according to the doctor, “there is a lot of corruption there when you pay the person for not reporting you” (confidential interview by telephone, Quito, Ecuador, February 25, 2022). In Ecuador, for this same interviewee, “those controls are what the country lacks; at times, they hide the cows from you and don’t tell you they have brucellosis” (confidential interview by telephone, Quito, Ecuador, February 25, 2022). While ideas make actors work together to address common threats, some stop them from doing so for selfish purposes rather than the greater good.

In addition, although actors agree or disagree with community, societal, institutional, or administrative norms, they bring forth an improvisational perspective of security governance in which ideas are inclusive. The case study reveals the idea of security on a grander scale in relation to multiple actors. An epidemiologist cares about a pathogen due to its resistance to antibiotics and the increasing threat to global public health. A military officer has a keen interest in someone weaponizing a biological agent, which means the official goes after the criminal in a counter-terrorist setting. However, both scenarios create the same effect: a pathogen that spreads rapidly around countries and people and is hard to control is considered a threat. In the United States, division appears everywhere from politics, vaccinations, power, money, class status, buying a house to rent, academics versus non-academics; even linguistics has now taken a beating: to some, the educational system has marginalized the use of words to fit particular norms, an endless list of divisions. So too enters the world of security, in which, as Colonel Patrick J. Mahaney, Jr. said, in the “United States, we divided out security and safety as if they are two different things” (interview with Colonel Patrick J. Mahaney, Jr., United States, February 14, 2020). To some individuals, security means people with guns, whereas safety involves guards, the fire department, or the building’s safety director. However, let us look at security from the perspective of Latin America, from the perspective of Spanish, a romance language. Security or *seguridad* intuitively provides us with a more holistic understanding of the problem and how to address it. We have separated the idea of security when a holistic viewpoint of security considers all aspects, such as biological, health, and safety-security. As this same interviewee pointed out, “The answers to some of what we're looking for in the national security realm come from different realms" (interview with Colonel Patrick J. Mahaney, Jr., United States, February 14, 2020). The Colonel added that it was "much easier to achieve cooperation, whether internal to the US, our allies, or even internationally, with people we are not partnered with or allied to" (interview with Colonel Patrick J. Mahaney, Jr., United States, February 14, 2020). Therefore, the idea of security between nation-states connects to collaboration, which depends on the *who* and is applied case by case. Security governance aspires to uphold the emerging health regime, which, in the process of surveillance, contains aspects of not being exposed to danger, an appearance of a secondary set of principles, that is, a security regime. The case study shows that although GLASS conducts a job more aligned with the coordination of the surveillance of member-states' AMR surveillance system, nevertheless, during the process of coordination, the institution monitors and controls the information through checks and balances. For example, the WHO-GLASS returns the same AMR data to the respective member-states for analysis, validation, and quality assurance checks if the data contain errors. Likewise, the WHONET database that contains the information ensures confidentiality and provides encrypted files before data pooling. Some argue that these are simply safety checks that do not rise to the level of security per se. However, if we follow the lead of the romance language of Latin America to include *seguridad*, safety and security interconnect. Why must we have a division even in the name of security? In this sense, the GLASS results in a more trustworthy form of surveillance. The idea of protecting the data is enough to make sure that the information presented publicly and coherently takes the same actions and relations between the actors toward the next level of safety-security. Therefore, a security regime operates within an emerging health regime.

Collective Purpose: Driven Momentum

The fifth feature of security governance involves a collective purpose and how actors interact. A lawyer knows the law, a doctor knows medicine, a plumber knows about plumbing, a mechanic knows about mechanics, and so on—an endless list of professional knowledge. When different industries come together and diverse experts collaborate and share information, doors open from all points of view to tackle an issue. For example, for a collective purpose, the greatest influential minds, Nobel laureates, gathered during the fifth Solvay Conference in 1927 to discuss photons, electrons, and quantum theory.

Similarly, the WHO has partners across many sectors to develop a global action plan to mitigate AMR (World Health Organization 2014). Likewise, during the COVID-19 pandemic, groups of global health actors such as the Global Fund, Unitaid, Wellcome Trust, the WHO, and private-sector partners launched a call for collaboration to accelerate the development and equitable global access to health technologies (World Health Organization 2020d). Furthermore, in engaging creative solutions, the actors mobilized a call towards interconnectedness and inclusivity, collective problem-solving, stakeholder connections, and shared knowledge and expertise (World Health Organization 2020d). Thus, collaboration empowers actors to use their talents for expression, achieve their collective purpose, and do things that benefit themselves and other actors and society.

The fifth indicator necessitates a collective purpose in the collaborative network of interconnectedness. Governance entails a system of rules (Rosenau 1992), and actions of "other members of the collectivity in an interdependent system" determine the rewards (Young 1992, 189; 1969). Governance maintains the collective order, the collective processes of rule, and helps to achieve collective goals (Webber et al. 2004; Rosenau 2000). Furthermore, security governance entails a "legitimacy of collective outcomes" (Holsti 1992, 50) in which "all broad issues required collective responses" (Rosenau 1992, 41). The purpose connects to the outcome of the process in the interaction of actors (Webber et al. 2004, 8). The WHO, a specialized UN agency, coordinates and directs diverse authorities to promote health internationally. The WHO provides a purposeful representation of worldwide health issues; connects people, partners, and nations to scientific evidence; and promotes health (World Health Organization 2022).

Furthermore, the WHO sets norms and standards, articulates policy options, provides technical support to nation-states, and shapes the global health agenda (Chorev 2012). In October 2015, the WHO launched GLASS, a collaborative effort of diverse actors to standardize the surveillance of AMR (World Health Organization 2017b), which provides a joint collaborative effort from participating countries and AMR regional networks. As its name indicates, the purpose is to foster national AMR and harmonize global standards, monitor selected indicators to estimate the extent of global AMR, collect surveillance data to estimate burdens, analyze and report global AMR data, detect resistance, and assess the impact of interventions (World Health Organization 2017b, 7). The WHO's strong alliance with reporting countries, regional offices, country offices, and collaborating centers has enhanced global surveillance and research. Therefore, concerning the study, GLASS as a collaborative initiative has brought diverse actors together with a common interest that drives the collective purpose to improve and develop new treatments for AMR.

Moreover, the WHO has launched projects such as GLASS to foster the importance of global health and surveillance of infectious diseases. In addition, official documents such as the IHR furnish the norms to define acceptable behavior to be followed by the participating member-states. Furthermore, due to an increasing threat to public health and its impact on the world economy, the WHO undertook various activities concerning AMR. For example, in 2001, the WHO issued the Global Strategy for Containment of AMR, which inspired regional and national AMR strategies (World Health Organization 2001). Furthermore, in 2008, the WHO established the Technical Advisory Group on Integrated Surveillance of Antimicrobial Resistance (TAGISAR), which advises the WHO on the surveillance of AMR in the food chain (World Health Organization 2017b). In addition, on the 2011 World Health Day, the focus of attention was AMR, and the WHO called for action by global stakeholders. Likewise, during the same year, the tripartite collaboration between the WHO, the World Organisation for Animal Health (WOAH), and the FAO claimed AMR as a priority health risk at the intersection of the human, animal, and plant ecosystems (World Health Organization 2017b). Lastly, by May 2015, the WHO's efforts to respond to AMR led to approval by the WHA of the GAP-AMR to tackle AMR at the global level

(World Health Organization 2017b). In particular, GLASS aims to address two GAP-AMR objectives: "strengthen the evidence base through enhanced global surveillance and research" (World Health Organization 2017b, 7) and "strengthen the capacity of all countries, in particular developing countries, for early warning, risk reduction and management of national and global health risks" (World Health Organization 2021d, 2). These norms serve to guide the member-states on how to conduct surveillance. The health regime, which establishes the rules, creates shared common principles based on the collective purpose. Nevertheless, part of the issue is raising awareness. Here is how one interviewee expressed the idea:

Confidential source. If more countries are demonstrating the problem, whether that's through GLASS or other existing surveillance systems, or through their hospitals or whatever and agriculture, if there's heightened awareness to the point where countries are implementing their action plans and they're developing rules and regulations around that in a sort of systematic way, then that could lead to more global awareness, recognition of the impact of antibiotic resistance, and push for the increased development of antibiotics (confidential telephone interview with a PEW executive, United States, January 29, 2020).

Any international effort on surveillance for AMR and infectious diseases includes countries from different regions coming together to address a common issue. The international health regulations are broad rules allowing activity from countries with varying resources and infrastructure built around AMR issues. Therefore, spreading awareness enhances the purpose, societal context, vigilance, and preparedness for a potential global health crisis.

The rapid increase of country enrollment in GLASS and active participation in a global surveillance system that monitors bacterial pathogens reflects a "collective understanding and engagement to support the global effort to control AMR" (World Health Organization 2017b, 135). The case study shows a 64% increase in country enrollment in 2018 compared to the first data call in 2017 (see GLASS data calls in table 3.2) (World Health Organization 2018a,5). In addition, the case study reveals that surveillance of AMR for bacterial pathogens of humans resulted in 42 members enrolling in 2017 by the end of the first GLASS data call and that the number increased to 94 in 2020 by the end of the fourth AMR data call (World Health Organization 2021d, 2017b). By May 2021, the number had increased to 109 countries and territories (World Health Organization 2021d). Therefore, more and more countries began working toward achieving the objective, namely, to report and systematically share data.

The actors arrived at a collective agreement on wanting good-quality microbiology laboratory data. The GLASS platform helps countries build their national surveillance involving scientists and different institutions the data from which usually go as far as peer-reviewed journals. The platform creates a collective purpose "to link all the efforts to collect the data to control the AMR" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). At the meso level, the information generated by the local institutions and scientists helps address the issue; however, at the macro level, governments responsible for fighting global AMR find it difficult to access data from local institutions. The GLASS platform connects diverse actors who collectively desire to control the threat. Thus, the mutually agreed upon principles also serve as a foundation to explore and expand on security.

The gray area of security versus data development, advancement of technology, and support to a collective goal creates tension.

Confidential source. You have to somehow find a balance between the possible good that might be derived from large datasets from research on various maladies and medical applications and so forth, in balance with discrimination, including, at crucial points, that the individual has the data about them as persons protected in that they ought to have a say in how the data is an informed consent (interview with a professor at the Rensselaer Polytechnic Institute, United States, November 9, 2019).

For some actors, the collective hope that turns toward figuring out how illicit agents turn pathogenic information into weaponized mechanisms takes time to unravel. This case study focuses on monitoring AMR in common high-priority bacterial pathogens that infect humans. For instance, the case study reveals that the reported median resistance to cotrimoxazole, a first-line drug to treat urinary tract infections, was 54.4% in the case of *E. coli* and 43.1% in the case of *K. pneumoniae* (World Health Organization 2021d). Similarly, GLASS reports reveal resistance to ciprofloxacin to be consistently high, as much as 43% in *K. pneumoniae* (World Health Organization 2021d). Although the results reveal a high resistance of pathogens, “you have to be able to process that pathogen into a weapon and that’s really hard in a way that is effective” (interview with Colonel Patrick J. Mahaney Jr., 14 February 2020). For example, theoretically, a person obtains the coordinates, feeds them into a bomber, flies out into a city, lets the device engage, and drops the bomb. However, many other biological and chemical weapons exist, such as ricin that have been processed. Thus, the GLASS pathogens are more effective in executing the end goal of the vector hypothetical.

This is how Colonel Patrick J. Mahaney, Jr. explained the implications of the scenario of North Korea developing a biological weapons program: “They’re probably working on enough bad pathogens out there that they do not need your eight pathogens from that one database. They are not going to want to have something that everybody’s looking at” (interview, February 14, 2020).

Actors with bad intentions desire something that is a nightmare scenario to the level of bringing on an apocalypse. They would want something like ricin and something even nastier than ricin. But, unfortunately, the 43%-54% AMR resistance level of certain pathogens does not rise to the fatality these actors aspire to attain for the masses. Regarding the WHO-GLASS system, the interviewee indicated:

Colonel Patrick J. Mahaney, Jr. The system is focused on an area that is a very common health concern that is hard to weaponize. Theoretically, it could be done, but frankly wouldn’t be worth it, and so, right there, it’s a great use of open-source intelligence to pick up what’s going on (interview, February 14, 2020).

For Lieutenant Colonel Arnel P. David, the results of sharing of open information regarding global public health through worldwide country surveillance are net positive. Regarding the GLASS-AMR global surveillance, the interviewee remarked that the system is a generally good thing.

Lieutenant Colonel Arnel P. David. Different states are collaborating with these new technologies and tools to share information to analyze across regions because, as we found out, with the coronavirus, these things spread fast, and if you don't have a way to map and figure out what's going on in these networks it will be there before you know it, and you can't deal with it (interview, February 10, 2020).

The impact of nonconventional threats is more extensive because diseases go beyond national borders. Likewise, nontraditional security threats are dangerous because of their ability to transcend national boundaries while undermining security measures developed by individual nation-states. Thus, the threat goes beyond the control of a nation when working with individualistic actions but collectively monitored to prevent the spread of a virus.

The case study shows a way of achieving a collective purpose to assess the spread of AMR and to strengthen knowledge through research and surveillance. Data collection, which the open-source or publicly available information from GLASS member-states facilitates, is the means to achieve the common good agreed upon by the actors. The information transforms into valuable intelligence. The collective and global public shares data to advance innovation. Nevertheless, security experts must protect the data shared by the worldwide collective from cyberattacks. Concerning global health issues, people generally all want to ensure public safety and avoid the spread of diseases that kill people, as Colonel Patrick J. Mahaney Jr. explained: "You're basically dealing with the same dynamics, except something much easier to understand, not the science of it but the case of it. Nobody wants people to die of horrible sicknesses" (interview, February 14, 2020).

This shared concern explains the rapid yearly increase in GLASS enrollments. The COVID-19 pandemic and its variants likely promote growth in other surveillance systems. Likewise, the post-pandemic may be characterized by the rise in the number of member-states enrolled in the GLASS network. The WHO considers the GLASS-selected microorganisms as common bacterial pathogens.

Colonel Patrick J. Mahaney Jr. People are waking up to the fact that these are hard to control. They are a threat, and they can get around very quickly. We all must be vigilant on this, and the good news is that it's something we can largely all agree on (interview, February 14, 2020).

Thus, actors promote the health regime because of the threat to global public health. The actors create the regime to channel disagreements in surveying communicable diseases so that the network can meet the common collective purpose despite conflicts among countries or other political issues. Therefore, the collective interest is better served by open collaboration among the actors with a common purpose. As a result, the collective is on the alert for the health and security of the people, the public, and the whole world.

The study illustrates how the WHO links actors in the collaborative network. Through an open exchange of information and data, the WHO's AMR surveillance project presents a platform for agents of continuity to respond to and address AMR surveillance and infectious diseases. Agents of continuity encompass entities, individuals, and structures that contribute to the ongoing response to and management of AMR surveillance and infectious diseases. Notable examples include the WHO, serving as a critical institution in building secure governance for global health matters; the GLASS surveillance system infrastructure, acting as an agent of continuity in the broader context of global health security, including its connections to non-member actors; the IHR regulatory framework, providing essential regulations for global health security; and various actors within the collaborative network, such as member-states, stakeholders, and public or private organizations actively engaged in addressing AMR and infectious diseases. The set or process of regulation through the IHR forms the basis of governance to secure the threats. The WHO builds security governance in global health matters as a critical agent. Specifically, as an institution, the WHO includes a regulatory component through the IHR. Likewise, the WHO-GLASS has a regulatory part through its organizational infrastructure, including links to non-member actors. Thus, the WHO engineer's security matters among various actors.

The spread of threat awareness organized by institutions such as the WHO has shaped the context of security governance. Alternatives that shape neutrality include the threat itself, which creates the drive for change, and institutions and executive leaders pushing the global spread of infectious diseases as a referent object higher on the national agenda. Examples of successful approaches to teach security governance include a framework where a multistage holder engagement of companies and governments creates a system in the event a threat, such as AMR or spread of infectious diseases, occurs. Actors prepare a wide broadcast of the crisis, thereby reducing the opportunity for the threat to spread and increasing awareness among affected actors. In addition, actors address global security threats by working together and rethinking the boundaries of actor roles.

The case study reveals how institutions and nation-states come together to form dominant security actors in the surveillance of infectious diseases. In this case, the WHO developed AMR global surveillance with participating countries that follow the established IHR. The research reveals how the WHO created a virtual heterarchy or multiple centers of power through its GLASS in AMR surveillance. The interaction of multiple public- and private-sector actors within the provision of security and diverse forms of institutionalization captures the building of a collaborative network. Likewise, more collaboration to address the issue develops as infectious diseases extend across continents. The process of regulation that guides international surveillance accompanies an exchange of ideas and data by an inclusive actor network toward a collective purpose.

Multiple channels connect societies, giving actors effective means of communicating with people about outbreaks of infection. The WHO shared the message of AMR surveillance with different groups through different channels, which include in-person or virtual meetings, mass media, enforced regulations such as the IHR, and information handbooks or guides such as the GLASS reports. In addition, the WHO provided security implementation in the GLASS reports to communicate security measures effectively. Thus, the case study shows that actors collaborated to promote a health regime for a common interest, such as eradicating infectious diseases. As the level of threat to security heightened, interactions between public and private actors increased. That said, for reasons other than science, such as lack of scientific awareness, hesitation, or fear of the unknown, some nation-states and institutions took time to interconnect and, at times, did not interconnect at all.

The case study also illustrates the importance of systems of rules, the interaction of actors, relations between actors based on ideas and concepts, and the purpose behind the drive to reach the goal. For example, actors need to have an awareness and understanding of how to implement ideas and arrive at decisions based on the collective common interest to prepare for and avoid a crisis. Similarly, a comprehension of the perceptions of reality allows fluid movements in the output of the perceived data, which increases trust in the actors' capabilities, such as institutions that implement the platform that provides the data and the technology that passes the information to the collective. Therefore, the data have a purpose; the gathered information leads to security strategies, priorities, and potential resources for different groups, such as intelligence and security officers, decision-makers, stakeholders, researchers, analysts, or scientists.

Moreover, during the development and deployment of technologies, stakeholders, actors in the private and public sectors, the research community, and policymakers develop ethical norms to govern conduct and ensure they use the technology platform responsibly. Bringing together stakeholders for productive discussions leads to recommendations and clarity on identified focus areas, such as the intersection of health and security. Therefore, without norms, emerging technologies, such as AI, are used by malicious actors in a way that harms by destabilizing fundamental aspects of civil life.

Civil society struggles with change and views modern technology with suspicion as the technology advances and evolves. Transparency becomes a significant issue in a system of security governance that is ever-more reliant on technology platforms. The information exchange surveillance databases facilitate fact production and provide the necessities for addressing infectious diseases and AMR resistance. The exchange also maintains an environment that encourages innovation in preparedness for future pandemics or global health crises. The institutions that create the technology data exchange platform decide whether the algorithms need modification for the health, safety, and security of its participating member-states. Intelligence monitoring does not stop at AMR or infectious disease surveillance. Still, it looks toward the type of platforms used during the information exchange process, even if the software is installed on a personal computer. This security governance goes beyond data and diseases and toward the digital space dichotomy. To err on safety includes looking for critical issues, such as potential cybercrimes or infectious diseases, in formulating mechanisms and a set of processes that guide international surveillance. Hostile groups have an increased ability to manipulate even the most innocent publicly available information, such as surveillance of common organisms, to control the digital space. Therefore, we must comprehend the system from all angles for intelligence and not just take what the platforms present at face value.

The purposeful construction of a security governance framework arises from the recognition that individual or national solutions are inadequate for tackling global threats like infectious diseases, which transcend boundaries. Security governance emerges as a response to the limitations of traditional policies, requiring a more dynamic approach. This process involves heterarchical centers of power, multiple actors, institutions, and the exchange of ideas that collectively drive momentum to connect societies and mitigate threats. For instance, the COVID-19 pandemic underscored the critical role of GLASS in aligning data-sharing practices with the emergence of a contemporary health regime.

Securitization theory becomes relevant as it examines how certain issues are elevated to matters of security, prompting nation-states and institutions to evaluate and implement enhanced security measures. The pandemic triggered emergency actions from a diverse array of actors, both human and nonhuman, within the network. These actions demonstrate the immediacy and interconnectedness required to address such global crises. The metaphor of a plate of poisoned food at a boardroom meeting illustrates this dynamic: actors are compelled to react instantly, prioritizing collective survival and problem-solving over individual hesitation.

In this context, actors ranging from nation-states to civil society play critical roles in shaping responses to modern-day pandemics. Their actions are not merely logistical but also emotional and discursive, reflecting the diverse narratives and perspectives that inform global collaboration. Theories like securitization help contextualize these responses, showing how the perception of threats reshapes priorities and drives the emergence of frameworks like health regimes. This interplay between theory and reality highlights how crises like COVID-19 and the growing threat of AMR not only stir immediate action but also reshape the conceptual and practical approaches to managing global health security.

Chapter 4
Discussion: Collaboration, Security, and Effective Preparedness

> It may be that while we think we are masters of the situation we are merely pawns being moved about on the board of life by some superior power.
>
> —Sir Alexander Fleming

In an environment filled with uncertainty, a sense of urgency arises, driven by the realization that failing to control the spread of pathogens will lead to illness and loss of life. This chapter extends the discussion on security governance measures presented in the case study in chapter 3. Although outbreaks may initially trigger hesitation and caution, the importance of international collaboration grows, emphasizing the need to overcome isolation. Nevertheless, the rapid global spread of an unforeseen pandemic gives rise to significant social, political, and economic upheaval. The urgency of being prepared for a pandemic is driven by the need to minimize the risk of disasters and brings together diverse actors who collaborate on pressing issues spurred by a shared interest. However, the interconnectedness of these actors also introduces security concerns in the realm of global data sharing. With that in mind, the following arises: Which actors comprise the network of collaborative efforts aimed at reducing risk and building resilience in the face of disasters? Is it possible to establish a health regime through a set of regulations or processes that guide international surveillance of infectious diseases? This chapter explores the objectives of the study, leveraging the insights from the case study to address the core research question, namely the reasons why security governance through a WHO OSINT technology database promoted a health regime focused on the surveillance of infectious diseases in the Americas between 2015 and 2021.

In answering the above question, the first objective is to open the black box of a health regime: this forms the first section of the present chapter, which discusses the strengths and weaknesses of instruments such as the IHR and GLASS. The section also looks at the relevance of publicly available information to the intelligence community and problems related to the culture and collective action in dealing with relevant factors such as infectious diseases. The second objective is to analyze the activation of security governance by an emerging and unconventional threat based on collaboration and open data exchange, which is achieved in three ways. First, it analyzes health and security issues in the areas of unconventional threats (AMR and COVID-19); second, it looks at *sui generis* disruptors that enhance or detract from the network; and third, it discusses the interweaving of health and security and the system of rules in the emergence of a health regime. The third objective is to explain why security governance works to secure a health regime in the surveillance of infectious diseases through OSINT. This chapter does so by describing (1) the different types of risks and challenges in using a database based on publicly available information, (2) the vulnerabilities and weaknesses of a system, and (3) the resources that enhance the global action plan on AMR and infectious diseases.

Regarding the actors relevant to such topics as the AI mechanisms connected to national security and intelligence analysis, this study considers, within the realm of health and security issues, the interconnection of human cognitive bias, algorithms, and advances in emerging technologies such as AI and its subset of machine learning (Sanclemente 2021; Fulmer 2019; McCarthy 2007). Machine learning, AI, and robotics manipulate the consistently changing innovation ecosystem. Could machine learning and AI capacities detract from or enhance the output of data exchange for analysts in the culture of the intelligence community? How does bias advance through knowledge production and education reinforced by technological advances to further cognitive development? Conversely, how do thought processes of research scientists influence the outcome of an AI mechanism? Diverse scholars interpret the cognitive process in analyzing intelligence (Wastell 2010; Thompson, Hopf-Weichel, and Geiselman 1984; Hendrickson 2008) because intelligence reduces uncertainty during conflicts or crises (Clark

2020). Similarly, "implicit biases in data and systems can arise because of unmodeled or poorly understood limitations or constraints on the process of collection of data" (U.S. Congress. Senate 2016, 16). Thus, advancing technology confers socioeconomic benefits and promotes innovation and creativity while stirring doubt, fears, and skepticism.

This section also addresses the security governance of a health regime and the changing scales in which the security governance occurs. The mixed health care economy based on R&D provides a blended economy in which collaborative networks of diverse actors become essential. This mix depends on "institutional legacies, the balance of political forces, and the changing economic and political conjunctures" (Jessop 2000, 21). Modes of information production land on a primary scale that actors decide on regarding social policies and economics. On the one hand, the importance of health innovations and tackling global issues such as infectious diseases and AMR signals its value to nation-states and individuals; on the other hand, as actors create regulations and security governance of data and diseases, "economic and social policies are politically mediated and the scales of political organization may not coincide with those of economic and social life" (Jessop 2000, 13). Therefore, the need for other supplementary mechanisms balances the economies of scale.

In addition, as technology develops and expands, it facilitates swift communication and physical movement of individuals from point A to point B, promoting collaboration and cooperation. Although the state maintains its primary role in the international system, leveraging the system with proper incentive structures, such as a health regime including a global surveillance system for infectious diseases, fosters institutional networking and collaboration among actors.

Opening the Black Box of a Health Regime

As mentioned above, the first objective in answering the main research question is to delve into the workings of a health regime beyond a superficial level by examining the black box and understanding its inscriptions.

To achieve this, the study evaluates the strengths and weaknesses of policy instruments that generate inscriptions to address nontraditional threats. Additionally, the study highlights the presence of a surveillance system that utilizes OSINT, or publicly available information, for monitoring infectious diseases. The study briefly explores the field of OSINT within the intelligence cycle, considering its relevance in addressing cybersecurity and nontraditional threats such as infectious diseases against the backdrop of emerging technologies such as AI and high-performance computing. Furthermore, this section includes an analysis of contextual information, taking into account other actors that both disrupt and enhance the network.

The black box helps to explain the unexplained. The operation of a black box can be reduced to a few well-defined parameters giving way to a swarm of new actors such as scientists, engineers, entities, firms, or social groups (Callon, Law, and Rip 1986). Likewise, cyberneticians use the word "black box" to refer to a complex set of commands (Latour 1987). In opening the black box of a health regime, security concerns exist because of outside unconventional threats that connect actors in the co-production of information. Therefore, entry into a health regime is through the back door of the new GLASS of AMR surveillance in the making and not through any ready-made technology.

During the analysis of the research question and gathering information, one can observe the implementation of diverse practices in the organizations, agenda, and regulations from the study. However, an important question arises: How are these systems of rules, known as security governance, conceived by actors? By opening the black box of a health regime, the installation of a security regime within it becomes evident. This additional layer of regulation requires an explanation. As stated by Guzzini (2011, 332), "it is important to open the 'black box' of why and how a particular outcome was actually reached." The identification of the actors involved in the network, their agenda, and the process by which they normalize issues within their specific agenda are key aspects to consider. The trajectory of this process is contingent upon the actions undertaken by the actors in the collaborative network.

Collaborative Grounding: Instrumental Influencers Governing the Security of Data and Infectious Diseases

This study uses the ANT as a point of departure to open the black box of a health regime. In opening the black box, a simplified entity and a network (Callon, Law, and Rip 1986) are examined to understand the forces that have shaped a health regime in the case study presented in the previous chapter. The study focuses on the complicated interplay between local, international, and nonhuman actors. The actor network theory considers the interactions between human and nonhuman actors. In this vein, the study sets out to analyze some neglected aspects of the black box of a health regime, such as security governance and its security measures. Opening the black box provides some insight into the effectiveness of open-source data within a collaboration. For example, the study analyzes the strength and weaknesses of boundary object instruments such as the IHR and GLASS; the relation between (1) the subject of the security threat and (2) AMR and infectious diseases such as and COVID-19; and how these instrumental influencers ground the collaborative process of interconnection. Regulations "serve […] the market and government through the code, since it has become a regulator, a definer of the terms in which places can be occupied in cyberspace" (Albornoz 2020, 53). Understanding the dynamics of these black-box entities and their instrumental influences is crucial for effective collaboration and informed decision-making in the realm of health regimes.

A scholar defines *cyberspace* as "the global network of interconnected information technologies and the information on it" (Segal 2016, 34). Likewise, codes condition how to access and interact with digital objects. However, subjects in a virtual world cannot change the regulations governing these spaces or demand a balance of everything the code takes away from them (Albornoz 2020, 53). While regulations imply control, participation by member-states in the Global Action Plan on Antimicrobial Resistance (World Health Organization 2015b; 2015d) allows the participants to be aware of the health regime.

This study addresses the IHR as a boundary object and instrument of "governance tool for managing outbreaks of new pathogens on a global scale, as they were revised in 2005" (Lakoff 2015, 301). According to one of the interviewees, "at the global level there are the International Health Regulations that is the most important document and the only legal framework that really affects all the countries and is the strongest legal document the WHO actually has" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Considering how slowly policy development and implementation in the global surveillance of AMR or other infectious diseases move many governments to implement a digital ecosystem for other countries to match. At an institutional level, the IHR, as an instrument of international law, create the health regime through their rules and principles. In response to deadly epidemics, the IHR bind every participating WHO member-state with obligations to report on events affecting public health (World Health Organization 2016a). The interviewee further added a strength of the IHR as a policy instrument and system of rules by noting that the IHR act as a blueprint and build the capacity needed to implement the IHR at a global level, leaving the responsibility to comply with the IHR with the member-states (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Another interviewee, Dr. Pablo Breuer, indicates examples of security governance or system of rules conceived by actors (governments, regulatory bodies) in response to cybersecurity threats that compromise the security of computer systems, networks, and data, including Europe's General Data Protection Regulation (GDPR) and the United States Privacy Act of 1974. Dr. Breuer is affiliated with the United States Special Operations Command of the United States Department of Defense and holds positions as a Senior Global Network Exploitation and Vulnerability Analyst, an Information Assurance Officer, and an Assistant Operations Officer (interview, January 31, 2020). Nevertheless, the IHR provide an interesting opportunity to set the principles which member-states agree to endorse and help implement. Getting the norms (regime) is essential, but the underlying infrastructure of how one enforces the norms of a nation-state is just as necessary. Through each country's ministry of health and multistate groups, the goal is to take these ideas and elaborate on them.

Moreover, the UN established a 25-member group of experts to address international laws on cyberspace called the Group of Governmental Experts (GGE) to advance responsible state behavior in cyberspace in the context of international security (United Nations Office for Disarmament Affairs 2021). This group of experts includes Brazil and Uruguay in South America. The world depends more on information and communications technologies (ICTs), including spaces that contain open-source data. The expert group reaffirmed the value of an "open, secure, stable accessible and peaceful ICT environment essential for all and requires effective cooperation among states to reduce risks to international peace and security" (United Nations Office for Disarmament Affair 2021, 6). Thus, instruments such as the IHR and GGE add to the maintenance of security and objectives in the surveillance of infectious diseases through information exchange in cyberspace.

Likewise, surveillance systems, an essential data-sharing instrument to detect and manage new threats to public health, include "informing policies and interventions, including stewardship and infection prevention and control" (World Health Organization 2020g, 3). In 2020, the COVID-19 coronavirus arose as the new target threat to national security and public safety. The global outbreak of the COVID-19 coronavirus pandemic reminded us that public-health events at one isolated location can spread rapidly to become a global crisis. The intelligence cycle includes the needs of the customer, planning, collection, processing, analysis, and dissemination (Clark 2020; Kovacs 1997). The intelligence community played a vital supporting role in public health. The more diverse the team of actors that coexist in the collaborative network, the better an organization performs and the closer it gets to de-escalating the national security threat. Controlling infectious diseases through public-health and AMR surveillance such as GLASS presents an effective way to help achieve monitoring and preparedness in preventing the spread of communicable diseases. In most systems for monitoring microbes, "countries provide routine surveillance data to multilateral agencies, which analyze and disseminate information on disease trends at the regional or global level" (Edelstein et al. 2018, 1324). One interviewee noted that the "surveillance standard is to help make empirical treatment policies" (confidential telephone interview with an Ecuadorian medical doctor, Quito, Ecuador, February 25, 2022). In addition, the case study reveals how GLASS, an instrument for global data sharing and knowledge production and a system of surveillance, raises awareness and expansion of ideas related to the AMR crisis. Other regions have established AMR surveillance networks including Latin America (ReLAVRA), Europe (EARS-Net), and Central Asia and Eastern Europe (World Health Organization 2017b). However, prior to GLASS, countries and laboratories did not coordinate a global surveillance system to standardize the collection of AMR data. The GLASS initiative created an intersectoral approach that enables harmonized global collection and reporting of AMR data, along with strict control and monitoring of infectious diseases. Another interviewee, a CDC official, added that surveillance systems complement each other "to provide a comprehensive understanding of known and emerging antibiotic resistance threats." Furthermore, the interviewee added that to prevent the spread and slow down resistance, the AMR surveillance systems provided "containment and prevention outbreak response, and drug and diagnostic development" (email interview with CDC-Info Official, Centers for Disease Control and Prevention, United States, February 17, 2020). For the neoclassical realist Colonel Patrick J. Mahaney Jr., U.S. Army (Retd.), international health regimes such as the case study make perfect sense: "My main interest as an American is that I think that the regime will help protect my country, my people and keep open the lines of trade and commerce, which I believe in, and it's a positive thing" (interview, February 14, 2020).

Nevertheless, the research shows the limitations of collecting routine public-health surveillance data, such as scientists ending up with significant biases. However, despite potential biases, scientists continue the surveillance on pathogens. For instance, the appropriate way for scientific actors to conduct a study includes obtaining random samples of patients. However, in the course of collecting such samples, Dr. John Stelling indicated, "from a scientific perspective, you want to control everything to make this a research project; the problem is it's not sustainable" (interview, January 24, 2020). Therefore, the data need to be targeted on a narrow subject with specific questions.

Public-health surveillance includes expanding more broadly, and while the research process contains levels of biases, Dr. Stelling added the need for "good quality science, but that's hard to do, and routine low-quality science still has value" (interview, January 24, 2020). The WHO validates GLASS reports rather than relying on open access to the underlying data since it comes down to the interpretation of data. Therefore, a scientist who interprets the data sometimes obtains data with biases and incorrect information. However, the underlying reality of the information remains, and epidemiologists realize the value. For instance, rather than choosing three high-quality hospitals, A, B, and C, in a country, it is preferable to collect data from all the laboratories in the country, an ideal scenario for surveillance. However, if hospital D is not part of a five-hospital network during an outbreak in hospital A, the out-of-network hospital D is unaware of the outbreak. Therefore, scientifically, routine data surveillance presents many testing quality and representation of results issues. Nevertheless, such problems do not slow the progress of science and the exchange of information between actors. Thus, while a scientist encounters issues with connectivity, lack of awareness of outbreaks, and biases during data collection in the surveillance process, this does not mean the information is not to be used, but instead that one needs to be aware of data limitations.

Managing controversies related to security in the collaboration to exchange open data includes dealing with concerns about obtaining new reports from low-resource countries because of the potential to miss quality microbiological results. However, greater appreciation of the limitations distinguishes routine public-health surveillance from high-quality, controlled, expensive, short-term research. As Dr. John Stelling noted, surveillance serves different objectives, such as "treatment guidelines, detection, advocacy, fundraising, baseline awareness, and situational awareness" (interview, January 24, 2020). Therefore, surveillance protocols help serve various objectives. However, individuals wake up to surveillance nightmares. For one academic interviewee:

Confidential source. The space that was once occupied by an open and resourceful research and debate within the general rubric of public interest, science and technology went into the inner spaces by politically naive, innovation-hungry, money-hungry, mainly white male nerds—they gave us the systems that we see today (interview, United States).

Nevertheless, for the interviewee, the alternative model is to also "open it up to the citizenry on how these things are studied, debated, voted upon, made public issues for people to vote on in regard to information systems that have the capacities for surveillance" (confidential interview, United States). Therefore, input from diverse expert sources has paved the way to strengthening and improving public health and encouraged good practice.

The world has moved into the digital sphere, and there is no going back. The COVID-19 pandemic has demonstrated that employers and employees conduct roughly half of their jobs online. During the peak of the pandemic in 2020, nation-states continued to collect and submit AMR data on pathogens. Implementing surveillance or monitoring systems such as GLASS requires input from several diverse departments. The departments communicate clear goals, processes, and rationales to avoid negative conflict. Where pushbacks occur, the WHO can act as a bridge between actors to resolve consequential conflicts. Nevertheless, surveillance systems in monitoring global AMR identify risk factors and guide policies. Therefore, GLASS provides the channel for global interconnection.

Intelligence Context: To Err on the Side of Openness Blanketed by Closeness

This section discusses the discipline of intelligence collection, OSINT, and the discipline's importance in the interweaving structure adding to the process of opening the black box. Emerging technologies and global health issues create challenges for the intelligence community during the workflow cycle. The issues drive the demand to access reliable computational platforms. COVID-19 presented unique opportunities for the intelligence community. For example, the Bureau of Intelligence and Research began its analysis with open-source and publicly available information, cables, and other reporting. Sometimes, the intelligence community moves forward with tasks regarding a workforce set at home. Intelligence operators and analysts have roughly 15-20 years of experience, speak multiple languages, and provide assessments based on open-source reporting, research, and geospatial information. However, as more information emerges, "problems of managing large and differentiated data streams and intelligence intensify" (Sanclemente 2021, 9). Turnover within the intelligence community arises from issues that the analysts encounter in working with an extensive, structured dataset.

Intelligence operations rely on a systematic process designed to meet the needs of decision-makers. This process involves defining stakeholder requirements, planning, collecting relevant data, analyzing and synthesizing findings, and disseminating actionable insights (Clark 2020). Stakeholders may range from national security leaders, such as the Secretary of Defense or the president, to officials within agencies like the DHS or members of military command centers. Each stakeholder's request informs the scope and focus of intelligence activities.

Collection efforts often involve diverse methodologies, including OSINT, which is defined as "information of potential intelligence value that is available to the general public" (Clark 2020, 178). Analysts face the challenge of balancing time-sensitive demands with the need for accuracy and reliability. To manage this, intelligence professionals prioritize sources that are both credible and accessible, ensuring rapid yet thorough collation and contextualization of data. This enables them to transform raw information into meaningful insights while addressing the unique priorities of various intelligence customers.

How can a pandemic and infectious diseases influence intelligence gatherings such as that on pathogens resistant to antimicrobials and on COVID-19? How do intelligence analysts pivot during a time of crisis? As life progresses, "big data provides massive amounts of information in a continuous stream that dissects and analyses a constant traffic inflow" (Sanclemente 2021, 3). How do security practitioners, policymakers, and professionals harness the power of OSINT via big data? This section focuses on the strength, weaknesses, and relevance of OSINT or publicly available information.

According to the U.S. Director of National Intelligence and the U.S. Department of Defense, open-source intelligence serves as intelligence produced from publicly available data which is collected and disseminated for the purpose of producing actionable intelligence (U.S. Director of National Intelligence 2006). Business intelligence, national security, and law enforcement units derive significant benefits or find utility in OSINT. In addition, analysts and researchers who use the information to answer intelligence requirements can incorporate OSINT into the analytic process. Likewise, OSINT techniques create an opening for nefarious actors, such as malicious hackers, as reconnaissance before launching an unlawful attack. Publicly available or open-source information, which contains a vast amount of information exchange, is a likely target of cyberattacks "because it has value" (interview with Colonel Patrick J. Mahaney Jr., February 14, 2020). Open sources contain information that is useful for criminals since they would want to de-anonymize the data. An intelligence expert interviewee indicated that open-source data are first anonymized but added that: "There are ways to de-anonymize health data that could be of interest to sell in the black market, and of interest for some nations who do not have access to it to hack" (confidential interview with a United States Special Operations Command Advisor, United States, April 10, 2020). Whereas the Colonel noted:

Colonel Patrick J. Mahaney Jr. Anything of value that can be accessed by cyber means is going to be a target, either to create a disruption, to seize it for ransomware purposes, or to tamper with it [For example, hackers can replace the original content with offensive materials or modify the visuals, thereby destroying the integrity of a digital resource.] Everything is going to be a target because somebody always figures out some incentive to do something bad (interview, February 14, 2020).

Thus, while the actions of criminal actors are illegal, the OSINT tools are a legal and valuable asset in assisting individuals with research, analysis, or identifying published work and data on public streams.

Open source for one academic interviewee means that the "source codes are open so that they can be used and adapted to a variety of applications that would not be possible if you had closure, proprietary rules and so forth" (confidential interview, United States, November 9, 2019). However, the path to promote a health regime stirs a need for open-source surveillance systems. One official remarked.

Medical officer at the WHO. If you really want to act upon any data, you must have access to the data, but also have a full understanding of the quality and reliability of the data. They build a mechanism on data collection, data analysis, and data use to follow rules of transparency when all the limitations and advantages are clear, but the most important thing is that they could be used for action by people who must know the data and could act upon the data (confidential telephone interview, Geneva, January 17, 2020).

Therefore, the WHO Medical Officer emphasized the necessity of open-source information, highlighting the importance of granting governments complete access to data to address critical human and public health issues, ensure data quality, and empower individuals to take informed actions based on the information provided.

In order to address the threat of AMR, the WHO created a mechanism to collect data through the development of GLASS while making sure that it is as transparent as possible. Could information on the internet, which is placed on a health care surveillance platform, be open? For instance, some information on a platform such as GLASS contains aggregated information, meaning the data are formed by combining several elements. In other words, anyone outside the WHO-GLASS realm and participating member-state groups do not have access to the raw data but view only summarized or aggregated data. While steering clear from defining open source, one executive noted: "All data that is cleared by a country to be published in GLASS is available for anyone who wants to see the data from the individual countries" (confidential telephone interview with a team lead of antimicrobial drug resistance at the WHO, Geneva, February 26, 2020). Thus, the participating member-states provide information to GLASS. In turn, GLASS representatives review the data which contain mistakes, return the information to the respective countries for correction, and then publish a summary of the findings on the GLASS website and in reports. According to the interviewee, GLASS resembles an open source but produces a frequent data call to participating member-states. "There are mistakes, and we need to go back to the country so they can correct it. Once all datasets are corrected, this is what's published. The GLASS reports present the summaries, and the individual details are available on the website" (confidential telephone interview, Geneva, February 26, 2020).

Therefore, on the one hand, the act of actors such as the WHO and GLASS posting information on the database for viewers to read and analyze comes under open source the moment the data are uploaded to the platform. On the other hand, in obtaining aggregated information, after finalizing the data with edits and corrections, the act of only publishing summaries does not necessarily amount to information obtained as open source.

Another official first considered the GLASS database to be an open source of information. However, when asked to define open source, the interviewee noted: "We prefer to use terms like 'publicly available' or just 'open.' There are so many other synonyms we can use, but basically to define the database, we use public domain" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Dr. John Stelling indicated that "GLASS database is not open," but that the WHO offers a free annual GLASS report in the form of a portable document format (PDF) to anyone in the world summarizing key findings which is "available through a public website" (interview, January 24, 2020). Furthermore, Dr. Stelling provided reasons why they do not want the information to be directly open by indicating the need for some degree of validity checking and issues of biases to correct the data but not represented in the results (interview, January 24, 2020). Thus, the interviewees correlated open source to synonyms such as public, free, or publicly available in providing information to the world.

Although the WHO interviewees noted that GLASS might not necessarily be open, when we think about security governance, the governing of data, and infectious diseases, the information that the WHO provides through GLASS and its reports is open and available to other groups such as intelligence analysts. Therefore, during intelligence gatherings, the research aims to be inclusive. Nevertheless, according to the interviewee who was an intelligence expert, "when you add many pieces that are in different parts of the open-source world and you put them together, that's where it could become a risk" (confidential telephone interview with a United States Special Operations Command Advisor, United States, April 10, 2020). Thus, depending on the targeted assignment, the data are a source of accessibility in analyzing threat levels to fulfill intelligence requirements.

However, the WHO indicated that the initial layer of data sharing is not open information to the public because they had to review and validate the data first, but actor action illustrates a form of control. Dr. John Stelling indicated that "there is a broader questionnaire, and the result of the broader questionnaire is not in the public report" (interview, January 24, 2020). Once the WHO's AMR division believes that its data are adequate to release to the public, the data become reliable. What is trustworthy and reliable when an institution opens the results as they are but only after analyzing the data? This type of information watchfulness also translates to controlling the output. Those in control of these spaces, such as in collective repositories of information, "can *de facto* exclude or include relational networks, which allow the imposition of norms" (Brousseau, Marzouki, and Méadel 2012, 29). The control of data prior to official publication creates a security actor. This feature of the security process within a health care setting is a method of crisis management. Therefore, the set of norms (a security regime) appears by controlling the information space before placing the health data in an open space.

Although the WHO-GLASS looks to provide trustworthy information, the system excludes information that WHO staff believe needs to be even more so. These means of data control offer a new layer of the power to control. Even if the actor has good intentions to make sure the preliminary reports before publication do not look out of place, we do not know the politics behind the purposeful choice because it is part of the black box, and only the WHO knows it. Since "human minds create new algorithms, code systems, or develop rules" (Sanclemente 2021, 7), only the WHO has designed the algorithms to analyze the data. In the present case, the WHONET software contained algorithms rather than AI for detecting outbreaks. We will likely never know with certainty the actual position of products of GLASS reports and the WHONET database since the research scientists who collect, analyze, and present the data only need sufficient certainty to meet their objectives. The actors will reach a point at which they consider the results of their product model to be acceptable. As GLASS reports are made publicly available or open to the world, those who reveal the information do not need to pursue it until the next round of reports. The product continues to be used by researchers until growing doubts about its accuracy, such as when additional member-states enroll and submit new AMR data, lead to re-opening the black box of the health regime and revisiting the assumptions behind global surveillance on AMR. If the algorithms are not open, there is a layer of opacity in deciding which layers are open to the public and which ones are not since not all that is open is genuinely open. Thus, unrestricted actors take publicly available or open-source information with a grain of salt and caveats since the original creator conducts edits behind the scenes before public transmission.

In addition, Dr. John Stelling, a medical doctor and co-director of the WHO collaborating center for surveillance of AMR indicated that the WHONET tried to integrate some elements of data mining (interview, January 24, 2020) and has worked with the Waikato Environment for Knowledge Analysis (WEKA), an open-source software (Frank, Hall, and Witten 2016; Hall et al. 2009). Recognized as a landmark system for machine learning and data mining, WEKA provides a toolbox and a framework to learn algorithms and reduce the uncertainty of data manipulation and scheme evaluation (Hall et al. 2009). However, what is the best algorithm? Dr. Stelling added that with multiple hospitals, each hospital uses different algorithms which "may not be the same algorithms that work the best but depends on the volume and underlying variability" (interview, January 24, 2020).

Moreover, different communities within the information ecosystem operate in the context of involuntary radical transparency, which "refers to a state of unintended data availability or openness" (National Academies of Sciences Engineering and Medicine 2015, 3). Analysis of data and insights are crucial for intelligence community agencies to perform their mission. Analysts obtain insights from a combination of data from many sources as the data volume increases and the data interconnect. In addition, there is an increasing need to collaborate across agencies, industries, and academia. Security-relevant data helps balance the risks associated with information sharing against the benefits of sharing the data.

Issues of Data Sharing: Collective Actions of Topic-Relevant Actors

An active community of data sharing depends on a sophisticated interconnected network of mutual collaboration. Science is just beginning to unravel how data ecosystems communicate. The preceding section focused on the need for OSINT and surveillance systems in an era of radical transparency as traditional security loses its effectiveness. When individuals log into a network and release their data for any service, it is akin to throwing a bottle into the sea-no one knows where the bottle will end up. Thus, the data become anyone's property. As a result, data floating around the information ecosystems, with no holds barred, present heightened avenues for security questions. What do actors consider to be a threat to national security? When do the data become a national security issue? How is this same mechanism used for health, and why does it become an issue of national security? What is the importance of securitizing certain matters? In opening the black box of a health regime, this section discusses the collective actions of topic-relevant actors such as infectious diseases, cybersecurity, and emerging technologies. This section also discusses security concerns posed by these nontraditional threats in data sharing.

Technology infuses every aspect of life, whether agriculture, such as payments to farmers in rural areas, or data science advances that transform every part of our lives. It is essential to be able to operate globally. This study investigated how the removal of borders, along with the emergence of epidemics and the sharing of data, impacts security, particularly considering the potential for shared data to be exploited for malicious purposes such as biological attacks and hacking. Regarding data sharing, a medical officer at the WHO remarked that the "WHO believes there should be no barriers to data sharing" (confidential telephone interview Geneva, January 17, 2020). There is value in being connected, but our social values must be reflected in technology. Society needs to hold technology companies and organizations accountable for the promise of their products and how they use them in practice. Likewise, actors need to be accountable for how they use products, which includes focusing on the greater good of combating infectious diseases and keeping in mind the type of data to distribute so that they do not fall into the wrong hands.

However, "national security means different things to different people mainly because of the changing nature of the threats and security risks" (American Association for the Advancement of Science, Federal Bureau of Investigation, and United Nations Interregional Crime and Justice Research Institute 2014, 10). For instance, Colonel Patrick J. Mahaney Jr. indicated that the "threat to national security sometimes manifests itself as a threat to public safety" (interview, February 14, 2020). Meanwhile, another interviewee noted:

Dr. Nancy Campbell. I think of national security as a political discourse that has done a lot of damage in our country because we often mobilize under national security to not share information, excluding people, policing, and surveilling populations that we think of as threatening (interview, November 12, 2019).

Another perspective on national security emerged from an interviewee who asserted, "anything that endangers the health, well-being, or internal affairs of a nation-state is a national security threat" (interview with Dr. Pablo Breuer, United States, January 31, 2020). Conversely, an intelligence expert emphasized the significance of education in national security, stating that "if we don't have a population who can critically think than we don't stand a chance against disinformation" (confidential telephone interview with a United States Special Operations Command Advisor, United States, April 10, 2020). According to the interviewee, educational failure places a country's safety and future economic prosperity at risk (interview, April 10, 2020). Meanwhile, for a security expert, there has been a paradigm shift in understanding security since the seventies, when "it was a military-oriented definition and the concept of national security was mainly in terms of military threats" (confidential interview with a security and sustainable development consultant, United States, November 4, 2019). Today, national security is all encompassing, and the interviewee remarked that "economic security is a very vital component of the concept of security and within the subset of economic security you would have health and health security" (confidential interview, United States, November 4, 2019).

National security issues fundamentally threaten the state's survival and are not simply political problems for governments but work in lockstep with allies and partners who share a common interest. For example, securitization functions with a political concern that becomes a security threat when actors such as states securitize it. In addition, potential issues deriving from bias in emerging technologies have national security implications with infectious diseases and cybercrime. Therefore, for intelligence analysts, understanding the consequences of human bias helps shape how analysts obtain, analyze, and deliver information to customers.

The world forum traditionally included security threats such as terrorism and climate change on the global agenda. However, threat topics have evolved to where bacterial resistance appears in the world forum, and AMR is one of the top ten global threats to public health (World Health Organization 2020b). Therefore, AMR has become more critical because of pressure from international organizations. A number of interviewees discussed the idea of threats and national security. Depending on the context, they deemed threats essential to certain nation-states while undervalued by others. As one official indicated, "the communicable diseases caused by multidrug-resistant pathogens are more dangerous than others and one of the recognized health security threats that remains in the yearly list of global health challenges" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Another interviewee considered AMR a national security threat since it is "within the groups of threats worldwide" and in Ecuador, "right now, the threat is the multidrug-resistant *Salmonella infantis*" (confidential telephone interview with an Ecuadorian medical doctor and temporary advisor on antimicrobial resistance at the PAHO, Quito, Ecuador, February 25, 2022). The WHO produces a list of the most important health threats (World Health Organization 2017d). One WHO official explained that "communicable diseases are a threat by themselves when pathogens become resistant to the accessible drugs" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). For another interviewee, national security threat includes "what's known about the means of transmission and the extent to which one can have a reasonable prediction that this malady is crossing national lines" and added: "I would consider a national security threat an infectious disease of some kind that was known to cross borders" (confidential interview, United States, November 9, 2019). Likewise, another interviewee explained that one in three individuals who travel out of Ecuador returned with their intestines full of bacteria (confidential telephone interview, February 25, 2022). Therefore, a risk develops since the infection already colonizes in the intestine once the patient gets sick, and people bring pathogens back to their home country when they travel abroad. Thus, according to the interviewee, pathogens colonizing the human body while traveling abroad present a national security risk to the country once the citizen returns home suffering from specific diseases that affect citizens while traveling (confidential telephone interview, February 25, 2022).

Another health and security threat is related to the control and treatment of infectious diseases, evidenced as "the world is increasingly interdependent, and that human health and survival will be challenged, *ad infinitum*, by new and mutant microbes, with unpredictable pathophysiological manifestation" (Henderson 1993, 283). For instance, sanctions create the inability to obtain quality medical products necessary to address concerns related to AMR. An official interviewee emphasized the dangers posed by communicable diseases resulting from pathogens that evade effective control and treatment measures, stating: "For me, another health threat is the communicable diseases themselves caused by pathogens and problems with controlling and treating them" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). The interviewee highlighted the significance of surveillance data on antimicrobial resistance, noting, "the surveillance data on antimicrobial resistance collected is the data that the countries selling the antimicrobial drugs could interpret and see what are the gaps in the current situation" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Moreover, the interviewee drew attention to the grave implications of pathogens developing high rates of antimicrobial resistance and the ensuing challenges in accessing essential drugs due to sanctions, trade regulations, and other barriers which pose a threat to national security (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). In attempting to rush access to antimicrobials, faulty algorithms or skewed data present a challenge that adds to unmanaged security risks. Thus, removing checks of an unbalanced algorithmic formula allows more focus on disease diagnosis, detection, and preparedness.

Building a Health Regime through Security Governance

The complex interdependence of the shared goals among actors or participating member-states affects the actors' collaborative process. For example, the surveillance process of infectious diseases places a higher priority on shared goals than on the department or individuals. In other words, the focus is more on getting the job done (such as collecting the surveillance AMR data and sharing the information on a public source) and less on security or whether one discipline differs from another. Although arrangements form regimes "for sustaining and regulating activities across national boundaries" (Rosenau 1992, 8), various health and security issues arise: Who is being affected? What controversies exist between the collaboration involving different actors for data sharing in building a health regime? The key to interconnectedness is reviewing problems such as the economic and social costs and the need for regulations due to privacy and security concerns in building a health regime.

Issues in Health Security: Infectious Diseases Awareness from AMR to COVID-19

According to the Population Division of the United Nations Department of Economic and Social Affairs, as of July 1, 2015, the world population was 7.349 billion. According to the WHO, by 2030, one in six individuals worldwide will be 60 years of age or over, and by 2050 the world's population of 60 years and older will reach 2.1 billion (World Health Organization 2021a). Most of the increase leads to greater stroke rates, lung diseases, dementia, osteoarthritis, and hearing and visual impairments. In turn, the conditions increase markets for medical devices and health care. Despite the diverging national interests of individual players, actors "recognize in rhetoric and decision calculations a greater interest, a common good, and an obligation to do things" (Holsti 1992, 41) to tackle an issue. Likewise, AMR, a severe global health problem, affects different sectors, such as human health, animal health, the environment, agriculture, and trade. Many factors favor the selection and dissemination of antibiotic resistance. Inappropriate and indiscriminate use of antibiotics is one of the main factors contributing to this phenomenon and poor control of bacterial infection.

The WHO considers AMR a "global health and development threat" (World Health Organization 2020b, para. 1) and a "global health security threat that requires concerted cross-sectional action by governments and society as a whole" (World Health Organization 2014, XIII). As previously discussed, from the end of December 2019 to early January 2020, the WHO reported 44 cases of pneumonia patients of an unknown cause in China (World Health Organization 2020h). By January 2020, the Secretary of HHS determined the existence of a public-health emergency (U.S. Department of Health & Human Services 2020c), and the WHO declared COVID-19 a public-health emergency, characterizing the virus as a pandemic (World Health Organization 2020w). As the global pandemic spread rapidly, a natural phenomenon such as AMR emerged through the overuse and misuse of antibiotics resulting in the spread of resistance, ineffective treatments, and persistent infections in the body (World Health Organization 2017b). Therefore, the inappropriate use of antibiotics played a role in the emergence of AMR and increased the risk of spreading infectious diseases.

Team lead, antimicrobial drug resistance, at the WHO. All surveillance systems are there for public-health purposes, and they are linked. It's at a higher level that countries be made aware of the burden of tuberculosis (TB), the burden of HIV, the burden of influenza, malaria, common bacterial pathogens, and resistance of these common bacterial pathogens to antibiotics (confidential telephone interview, Geneva, February 26, 2020). Regarding health and national security, another interviewee said that "one of the top things to be concerned about is needing to have infrastructure in place to have the surveillance, but to have systems in place to address a variety of potential threats that are too critical" (confidential interview by telephone, United States, January 29, 2020). Moreover, although the participating member-states ratified the IHR, which require them to share information, another interviewee added that the "securities are jeopardized only when data are not disclosed in time and not really shared" (medical officer at the WHO, confidential telephone interview, Geneva, January 17, 2020). Therefore, actors place greater emphasis on larger infectious diseases as important issues in improving national security efforts.

Economic and Social Costs

Countries worldwide face pressure to reconfigure their health care system to rein in costs and deliver care more efficiently since "infectious diseases account for a large percentage of healthcare expenditures" (Figge 2018, 21). According to the Organization for Economic Cooperation and Development (OECD), the size of the nation-state economy varies based on the amount of health spending and economic growth. The OECD notes that the average share of health spending in GDP increased from 8.8% in 2019 to 9.7% in 2020 due to the pandemic crisis (OECD 2021). Therefore, health spending increased as the COVID-19 crisis severely restricted economic activity.

In 2019, before the COVID-19 pandemic, OECD nation-states spent approximately 8.8% of their GDP on health care (OECD 2021). For instance, in 2019, the U.S. spent most on health care, with 16.8% of its GDP. In Latin America, Brazil spent 9.6%; Colombia, 7.7%; and Chile, 9.3% of their GDP (OECD 2021). At the same time, countries such as the People's Republic of China spent 5.1% and India, 3.6% of its GDP on health (OECD 2021). By 2020, estimates of health care spending significantly increased to combat COVID-19. For instance, in 2020, countries spent an estimated higher percentage of their GDP on health care due to the pandemic crisis; for example, the United States spent 17% and Chile, 9.4% (OECD 2021). Thus, economic spending on health care escalated as the threat of the pandemic heightened.

Furthermore, the WHO and pharmaceutical companies have a common interest, including the use of high -quality drugs, access to medicines, and the protection of intellectual property rights. Nevertheless, the maintenance of access to and distribution of medicines presents issues or controversies between different actors in the emergence of a health regime. For instance, Dr. John Stelling noted that “the pharmaceutical companies are pushing the sale of their drugs, and WHO tries to push the sale of the cheaper drugs and alternative drugs” (interview, January 24, 2020). One general recommendation that he added was that antibiotics be made available by prescription to reduce the economic burden of health costs. However, the social cost of limiting access to certain medicines only through prescription orders is that people in low-resource countries would lack access to those medicines because they often do not have the means or the facility to obtain a prescription. Nation-states privileged with access to treatment, advanced technology, and transportation infrastructure have the ease of resources, but underdeveloped countries do not have the same luck (interview with Dr. John Stelling, January 24, 2020). Although the interests of different actors matched in this case, they had different objectives. The pharmaceutical companies viewed the issue from a commercial perspective, whereas the ministries of health had a public-health perspective. In general, the world views AMR and its influence on the market. However, the coronavirus experience reveals that individuals do not always think of the threat to national security, namely, that a pandemic and AMR resistance combined can destabilize the financial markets, which touches many people.

Global Surveillance: Regulation and Legal Necessity

The need for regulations such as the IHR, code of law, and their interconnected nature creates a balance between fairness in health innovations and acknowledgment of technology advancements while being aware of security concerns that conflict with those of other fields. Furthermore, “sharing public health surveillance data across borders has legal implications when the type of data shared is protected by national or international law” (Edelstein et al. 2018, 1328). No matter how well-intentioned both the parties are in presenting their case, the code does not enable health care or technology actors and recipients of the information to lead a life free from confusion. On the one hand, researchers and scientists need to filter, clean, and purge the data before sending them onto a publicly available or open platform. On the other hand, transparency allows viewers to find truthfulness and integrity in the information presented. The two worlds, health and security, are interconnected, but to accomplish both without taking one from the other is challenging. Linking both presents complications. During one of the fieldwork interviews, one respondent discussed the importance of regulations and unions between health and security.

Ecuadorian medical doctor and microbiologist and temporary advisor on antimicrobial resistance at the PAHO. We will have to educate, improve all official administration, have more technical individuals, have personnel who last and endure the governmental system, keep the technical parts, and make sure it does not change each time the administration changes, change the whole way of being political in the country, and create public policies that last over time (confidential telephone interview, Quito, February 25, 2022).

Balancing security measures and health innovation while addressing the international system's non-systematic, socioeconomic, and inter- and intra-relations provides significant meaning for primary actors. For example, setting a legal or scientific precedent has a "very important theoretical weight in most legal systems," as well as a vital practical weight (Wiener 1989, 107). Moreover, the marriage of health and security is a critical union to maintain in preparation for any novel issues threatening the family bond. Therefore, blending health and security is vital to bettering nation-states and civil society.

Medical officer at the WHO. Certain small countries believe that some manufacturers benefit from getting access to the data because they will start producing vaccines of antimicrobial drugs and then sell them back to the countries for a fortune. At the same time, of course, it is to be regulated, but if the countries don't have the capacity to do this themselves then they will have to share so some will be able to produce the vaccines, and this is really a complex issue (confidential telephone interview, Geneva, January 17, 2020).

Actors who contribute information to a global surveillance system of infectious diseases raise concerns during the process of surveillance, particularly on how groups are identified and tracked. The case study shows that the WHO receives national aggregated data from the participating member-states and official NFPs. The same medical officer claimed that "they have no individual data in the database. So, it is absolutely impossible to obtain any personal information from the data" (confidential telephone interview, Geneva, January 17, 2020). Nevertheless, Lieutenant Colonel David cautioned:

Lieutenant Colonel Arnel P. David. If you know any kinds of data information from a country, whether it's their demographics or numbers and it might not be about individuals, but it could be quantitative data on things, it's going to paint a picture about a country's state and well-being (interview, February 10, 2020).

The research shows the intersection of health and security. The study further shows that a network such as GLASS collects aggregated data from participating countries; these data do not contain personal information on individual patients. In addition, through the regional country office, the member-states select the relevant data. Then, they pass the data to the GLASS network and are thus aware of its depiction in the final open reports. Nevertheless, the information is derived from country surveillance of selected pathogens. Therefore, data management is vital in protecting how countries are depicted during the analysis and ultimately placed in an open-source database.

Sui Generis Disruptors: The Interplay between Femtorisk and Influential Actors

This section explains the relevance of out-of-network actors because, at first sight, some actors appear to disrupt, slow down the process, or "move forward in a more controlled and deliberate manner" in the network (interview with Dr. Pablo Breuer, January 31, 2020). Actors such as malicious and non-malicious groups and internal and external groups slow the progress of AMR surveillance. For instance, non-malicious internal groups such as ethicists, doctors, engineers, or regulators indicate that a project is not ready or safe for production. In the preceding chapters, this study mentioned the various actors in the network of collaborative relationships. For example, the recent coronavirus pandemic showcased the complexities of international affairs and diplomacy due to technological, political, and financial developments. Unfortunately, two different but essential actors appeared to disrupt or slow down the collaborative surveillance network. The first were influential actors operating on extended time scales, constantly in the mainstream, and competing in the international system. The second were *femtorisks*, which are smaller actors than nation-state actors or international institutions that nevertheless catalyze substantial changes and pose challenges to international relations.

Sui generis disruptors, such as COVID-19 and the pandemic, enable us to understand global collaboration. We can look at COVID-19 as a non-human actor that disrupted the network on AMR surveillance, but also as an example of interconnectedness. This actor has a different connection pattern from other network actors. The COVID-19 pandemic influenced the global health system affecting the research, development, and management of other health threats such as AMR (Tomczyk et al. 2021). Although this node interrupts the network, it does not exactly hinder it. The actor network theory prompts us to consider all actors (human and non-human), and although COVID-19 presents a limitation of the network, it also illustrates the importance of network analysis, spurring innovation. For example, the CDC identified a high increase in resistant infections during hospitalization from 2019 to 2020: 78% in *Acinetobacter* and 13% in *Staphylococcus aureus* (CDC 2022c). These are two of the eight bacterial pathogens under study that affect humans. Thus, considering actors inside the network (WHO member-states) as well as outside it (COVID-19) helps to understand the construction of a network.

This study analyzes the influence of other actors that disrupt the network, such as the agency of China and hacktivists because "for every group to be defined, a list of anti-groups is set up as well" (Latour 2005, 32). Such counter groups also include "deviationist behavior, running counter to expectation" (Wolfers 1962, 13), and "dissent is inevitable in collaborative efforts" (Clark 2020, 92). The network analysis in chapter 3, documents, and observational research, and results from the data collected from the semi-structured interviews, indicate that these *sui generis* actors report no ties in the network during the scope of this study. Collaboration requires a common ground where a group of individuals has shared understanding and mutual knowledge of the problems (Feng and Kirkley 2020). However, due to technical, political, economic, motivational, ethical, and legal barriers, actors do not always collaboratively share surveillance data (Edelstein et al. 2018).

Nonetheless, an actor that does not appear to collaborate does not necessarily provoke a disruption in the network. Could disrupters work to glue the network together? Do disrupters enhance the dimensions of security governance? Consequently, practices, ideologies, and state actions that do not conform act as obstacles that disrupt the network or social order and threaten security. However, what constitutes conformity? The disruptors may have the correct norms or ideologies to address the threat. Thus, this section addresses the misalignment between open-access data sharing, non-participation in a global health surveillance system, lack of sharing information, and control of data.

China: The Influential-Disruptor Actor in the Surveillance System Network

As Bruno Latour (2005, 180) sagely remarks, the hyphen in an actor network "is not there as a surreptitious presence of the context but remains what connects the actors together". Context provides "another dimension giving volume to a too narrow and flat description" (180). For instance, the regime of China works to glue the network together. China's refusal to turn over raw data for analysis during the period under study frustrated members of the WHO (Hernández and Gorman 2021; Buckley and Lee Myers 2020). Likewise, only 15 member-states from the Western Pacific Region, including China and Hong Kong Special Administrative

Region (China), have developed their national AMR action plans (World Health Organization 2018a). As of early 2021, nine countries enrolled in the GLASS (World Health Organization 2021d, 2020g). By 2018 "only Japan, the Philippines, and the Republic of Korea reported AMR data to GLASS" (World Health Organization 2018a, 240), and until 2021 China continued to be unenrolled in GLASS. Therefore, context data such as China's potential resistance to providing information during the onset of the coronavirus outbreak and lack of enrollment in GLASS add another dimension to the collaborative network.

During the scope of this research (between 2015 and 2020), China was not enrolled in the GLASS network. Did the lack of enrollment by China or any other country disrupt the collaborative network? As already discussed, when asked about the country's exclusion, one official interviewee remarked that China's lack of enrollment in GLASS was due to technical difficulties (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). The WHO collects nationally aggregated data from small countries in which the data are easier to manage. However, how does the WHO interpret numbers from a country as large as China, with more than 1.4 billion people in 2019 (United Nations 2019b), that has multiple surveillance systems such as the China Antimicrobial Surveillance Network (CHINET) and the China Antimicrobial Resistance Surveillance System (CARSS) (National Health Commission 2021; Antibiotics Research Institute, Huashan Hospital Affiliated to Fudan University 2021; Wang et al. 2020)? The official remarked that "the calculation is different in [each] area. So, they are simply trying to figure out how we can make the data that is coming from China interpretable" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020). Due to the country's sheer size, "this is purely a methodological issue," the interviewee added, "there is nothing political" (confidential telephone interview with a medical officer at the WHO, Geneva, January 17, 2020).

Moreover, what would a country such as the United States not do to help China, medically or logistically, by providing medical information or epidemiological research? On the other hand, suppose part of a surveillance system connects to being political, and the system is used to further isolate, for instance, the Uighurs in western China. In that case, it is a different scenario in which actors are sensitive to not enrolling or contributing data to a global surveillance system. According to the WHO interviewee, China's lack of information sharing in the GLASS network was due to technical rather than political reasons. This is consistent with the view of the WHO Director General regarding China's lack of provision of data early in the COVID-19 case, which, according to him, "expressed the difficulties they encountered in accessing raw data" (World Health Organization 2021h, n.p.). As the case of China shows, technical and other issues prevent countries from accessing data on AMR and sharing them with others. A disruption in the process complicates knowledge production and sharing regarding a global pandemic or slows down efforts on the surveillance of AMR.

Nevertheless, distractions or disruptions in the network help understand the rhetoric of interconnection. In the grander scheme, the WHO brought the actors' lack of information sharing to assist in tackling a global health threat to the attention of the actors withholding such information. During the member-state briefings, the actors also expressed the importance and expectation of future collaborative studies and more comprehensive data sharing (World Health Organization 2021h). Does a country such as China understand the dynamics of global sharing and the expressions presented by the member-states?

Does the failure of a country's collaboration disrupt the entire foundation? The study reveals that the GLASS network continued with or without China as more and more countries continued to enroll in AMR surveillance. Nevertheless, as the coronavirus showed the urgency of global health threats, including an actor such as China in the network, a lack of information still enhances the international system even with a skewed network.

Hacktivists: The Femtorisks-Disruptor Actor in the Surveillance System Network

This study recognizes the significance of cybersecurity challenges to health information over the cyber ecosystem. Cyber security preparedness requires collaboration between different actors in the collaborative network, from nation-states to private actors and diverse sectors. However, "the globally interconnected nature of the Internet also means that cyberattacks have the potential to produce unpredicted and inadvertent problems far beyond damage to the intended target" (Segal 2016, 12). Likewise, the "challenges posed by increasing interdependence in the international sphere" include different actor interactions from the influential to the micro (Frank et al. 2014, 17356). Therefore, interdependence in the cyber ecosystem presents a paradox of relevant and comprehensive complex architecture.

The term *femtorisks* refers to threats "that confront international decision-makers as a result of the actions and interactions of actors that exist beneath the level of formal institutions or operate outside of established governance structures" (Frank et al. 2014, 17356). These semiautonomous agents behave and act in their local environment, a private club of disruption, per se. Furthermore, *femtorisks* are pictured as small fissures inside nodes grouped in different network topologies. These actors appear to wake up when the system typology needs a new alignment, and they decide it is time for a change, that is, a disruption. Their appearance is internal or external, regional or global, inside or outside the node or network, "but the effect is the same" (17356). Examples of human agents posing as *femtorisks* include aggressive financial innovators, rogue traders, groups of dissidents, or terrorists. Examples of nonhuman *femtorisks* agents are forms of "climate change, communications technologies, or socioeconomic globalization" (17356). This study includes hacktivists as *femtorisks*, particularly bad hackers that create systemic changes. Negative hacktivists present invisible risks that do not appear until after the system's exploitation and damage. Therefore, these actors alter the interactive dynamics between social events, international relations, and human interactions.

An essential part of the study is to differentiate between the three main types of hacker groups by intent and capabilities since not all hackers are criminals. On the one hand, there are ethical hackers (white hats) that use their skills to defend against a threat. A second type of hackers, known as grey hats, sometimes operates legally and other times illegally. The grey hats, for random reasons such as boredom or curiosity, find ways to hack into computer networks without malicious intent. On the other hand, evil hackers (black hats) with malicious intent to steal sensitive information cause chaos by accessing a secure network without authorization. For instance, black hats submit suspicious email messages to companies masking them as institutions, otherwise known as phishing. These actors exploit "unexpected and unknown vulnerabilities in networks to wreak damage and destruction" (Segal 2016, 25). Victims unknowingly click on the links or attachments through the method, believing the email to be originating from the institution. As a result, malware installs itself in the computers, and criminals obtain sensitive information, such as passwords and usernames. In 2020, black hats and cyber scammers increased their presence by taking advantage of the vulnerabilities of the coronavirus pandemic. In one instance, the WHO encountered a situation where email addresses and passwords associated with their organization, as well as those of numerous individuals involved in addressing the novel coronavirus, were exposed online. While the leaked login details did not pose a direct threat to WHO systems, an older extranet system, utilized by both present and former staff members, as well as partners, was affected by the incident. In response to the situation, the WHO took measures to mitigate risks of potential impersonation by implementing an email security control known as domain-based message authentication, reporting, and conformance (DMARC) (World Health Organization 2020c). This implementation aimed to minimize the adverse impacts of impersonation incidents. Nevertheless, as Dr. Pablo Breuer indicated, "certain adversaries, regardless of whether they are individual actors or hacktivists or a terrorist group or nation state, can have these effects on how we are moving the ball" (interview, January 31, 2020). Therefore, the WHO implemented DMARC to counter fraudulent messages.

Disruptions form part of the various *dispositifs* and boundary objects in connection to the GLASS network. These changes pose great challenges to the security governance and management of support systems for global public health. These dissident players heighten the level of security and how actors (both institutional and sovereign) continue to create information exchange platforms through open-source avenues. Some actors' pushback and disruptive manner provide reinforcement mechanisms to improve the system of rules or processes. Hacktivism always presents a risk, but with proper checks and balances, individuals quickly realize, for instance, that the data submitted to a global surveillance system from a health care institution located regionally or abroad were different from the data initially submitted. Quality assurances and quality data control assist in double-checking the information transmitted. By having active community participation in the surveillance system, especially during the information exchange, disruptors such as black hats are red flagged. The implementation of a cybersecurity system such as WHONET (O'Brien and Stelling 1995) has the advantage of being installed on personal computers, ensuring protection from potential cyber predators. Therefore, femtorisks allow actors such as decision-makers, intelligence analysts, security experts, or the military to understand that not only large influential actors interrupt the system but also smaller ones. Thinking outside the box allows for greater examination and interconnection of thought processing and building.

Benefits: Security Governance Assessment

The value of security governance, or a system of rules created by actors to ensure safety, increases when a pandemic brings isolation, uncertainty, and confusion. Governance prevails in the "lacunae between regimes" (Rosenau 1992, 8) when more than one regime overlaps. Security governance pretends to control both the disease and the data. Where a health regime and a security regime coexist, governance accommodates competing interests. The economic scales shift through the actions of diverse actors. Therefore, this section discusses the benefits of economies of scale in the security governance of open data obtained through surveillance of infectious diseases.

Moreover, this study shows the influence of technological innovations using surveillance mechanisms of infectious diseases. Would technological advancements tip the economic scales in favor of better production? How do state actors benefit from large institutions, such as the WHO, during the exchange of open-source data? Finally, how does a collaborative network benefit from a set of processes and institutions that guide the international surveillance of infectious diseases? This section builds on the case study in chapter 3 discussing the dimensions of security governance to assist in answering these questions and assesses the benefits of security governance by analyzing the concept of economies of scale, technological influence, and heterophily.

On the one hand, collaboration is more likely when actors are aware of a threat, as awareness fosters a shared understanding of the urgency and necessity for collective action to mitigate risks and address vulnerabilities effectively. Nonetheless, upon reflecting on theories and countering the liberal institutionalism theory, this research shows that when an unknown threat, such as the COVID-19 coronavirus and its variants, breaks out, the influence of nonstate actors decreases whereas that of nation-state powers increases. These fluctuating state and nonstate actions emphasize a realist theory. On the other hand, under realist theories that are "avowedly rationalistic" (Keohane 1988, 381), reactionary isolation to a pandemic brings inward attention, which brings the focus on nation-states. Thus, the security of a country goes beyond the safety and security of civil society and leans toward a selfish act of power and control.

Focusing on national security interests and the safety and well-being of their citizens, nation-states maintain and nurture outside connections to reel in a more progressive liberal institutionalism theory. The idea of interconnection is necessary for the cycle of social, economic, and political healing. An interweaving and collaboration of actors' movements comes about through the connections; moreover, in addressing COVID-19 or the next AMR-type pandemic, fixing the issue at a collaborative level shifts the economic scale. A healthier civil society stimulates the economy; one country alone does not solve the issue. However, collaboration between institutions and private actors contributes to the balance of scales and actions of diverse actors.

Economic growth stems from an innovative environment for different nation-states. Moreover, an essential part of the developmental process is derived from scientific and engineering contributions. Therefore, a collaboration of diverse actors intersects with the push toward economic growth. At the crossroads of economic growth and biological sciences is the bioeconomy. The White House Office of Science and Technology Policy defines bioeconomy as the "use of research and innovation in the biological sciences to create economic activity and public benefit" (The White House 2012, 7). In 2016, bioeconomy accounted for approximately $959.2 billion, or 5.1% of the U.S. GDP (National Academies of Sciences Engineering and Medicine 2020), 10% of the industrial GDP of Ecuador (Zambrano 2018), and 15.4% of the GDP of Argentina (Food and Agriculture Organization 2018). Therefore, the intersection of the economy, data, and biological materials provides space for innovation. In addition, different industry actors, such as health care and defense, have an interest in developing strategies for bioeconomy. Thus, strategic security measures also emerge as the bioeconomic sector grows.

Benefits of Balancing the Economies of Scale

The WHO reported, as of December 9, 2021, approximately 268 million confirmed cases of COVID-19 and 5.3 million global deaths (World Health Organization 2021g). As to AMR, more than 35,000 people die each year because of more than 2.8 million antibiotic-resistant infections that occur yearly in the United States (CDC 2019a). The study shows the difficulty in calculating the economic cost of antibiotic resistance in the country. However, "infections require extended hospital stays, follow-up visits to healthcare providers, and the use of treatments that may be more costly and potentially more toxic" (CDC 2019a, 5). Whereas the economies of scale depend on the meeting point of the national economy, state, and society, and the survival of nation-states as sovereign bodies, the structure has weakened, and the national economy has been undermined by an increase of multi-tiered networks (Jessop 2000). Strengthening cross-border collaboration in the Americas has brought a scale economy of investment and innovation to health care facilities, more cost-effective expansion of security mechanisms, and global public-health benefits. Security translates into cooperative efforts in economic development to generate an environment of interdependence in a complex system. The scale of collaboration increases with the size of the institution. The greater the institution's size, the higher the number of its associations with other actors. The number of collaborations by agents of continuity, such as participating countries, medical experts, academic experts, and R&D teams, increases as the institution grows. The WHO launched GLASS in 2015, a relatively new network. However, since its launch, GLASS has expanded in coverage. As of 2021, within five years and in the middle of the coronavirus pandemic, GLASS enrollment had increased to 109, including countries and territories worldwide. These actions illustrate the economies of scale: increasing the output lowers the threat level as more and more information is disseminated and exchanged.

Similarly, the more actors produce, the cheaper it becomes to obtain an outcome. However, the scale reaches a point where it becomes more expensive to produce, such as in the case of the surveillance of infectious diseases. Along the same lines, in the present case, adding more participating member-states to the surveillance network increases the scale of the agenda. In certain circumstances, at a macro level, resolving global conflicts, such as combating infectious diseases, generates higher costs for a state. Nonetheless, from the perspective of AMR, the study shows that collaborative efforts add little cost since the GLASS platform creates the foundation, and the IHR provide the rules. It only results in greater profits: global surveillance of AMR through the collaborative efforts of diverse actors. Therefore, the probability that the GLASS affects human security is decreased.

Nonetheless, from a technological perspective, a large institution such as the WHO, which has more prestige and funding, can adopt production technologies, for instance the GLASS platform. On the other hand, collaboration places the economies of scale at risk in terms of transaction costs. Participating countries can contribute to knowledge production and use the platform, but smaller member-states need more resources to afford participation. However, large countries may have the finances to invest in the surveillance system in R&D for infectious diseases. Although smaller countries do not achieve greater economies of scale, they achieve external economic scales through collaboration and interconnectedness. Likewise, on a geographic scale, smaller countries benefit from a shared platform of open information by contributing to the platform, which, in turn, assists in their R&D in response to bacterial pathogens in their respective countries.

Moreover, medium enterprises and start-ups drive a large part of bioeconomy, and their ability to influence licensing lands on a different scale than their traditionally large corporate firm counterparts (National Academies of Sciences Engineering and Medicine 2020). Concomitantly, "the cost of AMR to the economy is significant" (World Health Organization 2020b, para. 5). Global actors react responsively to the power dynamics of economies of scale since "misuse and overuse of antimicrobials are the main drivers in the development of drug-resistant pathogens" (World Health Organization 2020b, 1). Antibiotic resistance affects the agriculture, veterinary, and health care industries. Therefore, the ability of actors to respond in tackling a health issue drives the scale of reactivity.

Benefits of Technological Influence

The theory of path dependence provides insights into the tendency to follow a familiar course of action, with the expectation that accumulated random variations along that path will yield improved outcomes (Keohane 1988; David 1985). Path dependence suggests that the sequence of economic changes, shaped by chance or remote events, can significantly influence eventual outcomes (David 1985). Nevertheless, there are situations where it is illogical to persist on the same trajectory based solely on historical precedent. The 2020 coronavirus pandemic serves as a stark reminder that continuing along a familiar path in the hopes of developing a new approach may prove ineffective.

Concerning the surveillance of infectious diseases, "path-dependence occurs under conditions of increasing rather than decreasing returns" (Keohane 1988, 389). Chapter 2 illustrates the positive externalities of the contributing actors, enhancing the advantages of a collaborative network from the convergence of an established standard. For example, GLASS, an instrument of production, depends on the software created by the WHONET (O'Brien and Stelling 1995). The IHR, as established international standards, lead the process that guides the member-states toward their collaborative nature. Although technology is neutral, we cannot call technology inclusive or non-inclusive. The rapid pace of technological progress suggests that inclusivity depends on how actors implement a given technology. For instance, global health professionals use electronic health records to help physicians track patients' health, check for possible harmful drug interactions, and provide medical support. Thus, the digital divide is a cause of concern for poorer countries, given the lack of affordable crucial technology in the health field.

Global Efficiency: Appreciating Heterophily to Collect Data from Diverse Groups—Amor Al Diferente (Love of the Different)

As we have observed in this study, actors recognize the value of acquiring a diverse collection of data from various groups, and their actions contribute to the promotion of a health regime. Similarly, according to Zacher (1992), "progress toward greater collaboration in security, economic, environmental, and social fields depend on one development—the continued reluctance of great powers to embark on war with each other because of the costs of nuclear war" (Zacher 1992, 61). The preceding sections have highlighted how technological advancements have led to unprecedented economies of scale for global actors, thereby resulting in enhanced global efficiency. Therefore, this section explores the concept of heterophily, which emphasizes an affinity for diversity. It showcases how different *dispositifs*, boundary objects, and actors collaborate and connect to GLASS, exemplifying their collective efforts and interconnections toward achieving common goals.

The study shows a tendency towards heterophily, where actors from diverse industry backgrounds, such as security, health care, intelligence, and military, collaborate. This heterophilious collaborative network is better able to spread innovation and tackle security threats through surveillance and information exchange via open-source or publicly available information. Although moving data offline or outside a shared network is the ideal, or a dream, for security experts, the hindrance makes data less accessible for innovation. Thus, more data exchange and actor collaboration are needed to speed up progress and innovation and identify bad actors.

In conclusion, an acceptance of security governance seems possible in the presence of strong technological interconnection, economies of scale, and an appreciation of the inclusion of different actors in the grander scheme. Institutions have scalable projects that influence the economy. As large institutions form greater collaborations, the impacts of the collaborations are increasingly visible and growth is faster. Why share information on an open-source platform with potential risks to an actor's security? Why contribute to a collaborative network in the surveillance of infectious diseases where unmasking opens the doors to other security threats? Transparency and data exchange offer avenues for innovation. An increased number of participating member-states and other external actors act as agents of continuity, which increases the chances for preparedness and response to present and future threats to their security (safety). Thus, following a set of processes guides the international surveillance of infectious diseases and benefits the larger picture of global health, security, and well-being.

Alignment of Managed Sharing of Big Data

This section focuses on the third objective of the research and discusses why security governance works to secure a health regime in the surveillance of communicable diseases through OSINT. The analysis highlights the significance of identifying risks, challenges, vulnerabilities, and resources in this context, considering the interdependencies between multiple actors involved in data exchange. By establishing a system of rules in response to threats, the exchange of data and utilization of publicly available information for disease surveillance play a crucial role in ensuring a secure health regime. Moreover, the implementation of a surveillance program that effectively identifies risks, vulnerabilities, and resources can serve as the driving force behind the protection of health. Collaboration between various actors within a regulated framework facilitates the exchange of information, reinforcing the efficacy of security governance in safeguarding the health regime. Consequently, this section is divided into three parts: an examination of risks and challenges associated with using a database containing publicly available information, an exploration of exploited vulnerabilities in applications, and an analysis of resources that contribute to informed decision-making, including support for the global action plan on AMR and efforts to combat infectious diseases.

Risks and Challenges

This study illustrates how risks and challenges arise in using databases containing open information. This section discusses cyber biosecurity, bio-economy, data manipulation in algorithms, and the repercussions of data being placed in the wrong hands.

Negative Outcomes: Risks of Exposure to Threats and Open Data Technology

The risks of exposure to threats when multiple actors provide information on an open-source surveillance platform, and data sharing, generate actions which result in a negative outcome. Acceptable and unacceptable risks exist. As Dr. Pablo Breuer indicated, "You want to do things in a way that you're not taking unacceptable risks, and the acceptable risks that you're taking are well known and well understood, and it's deliberate" (interview, January 31, 2020). Understanding the risks helps groups, such as the intelligence community, to consider how much to trust the results based on data coming from open sources. For example, publicly available platforms such as the GLASS surveillance reporting database, on the one hand, contribute to the building of a health regime but, on the other hand, present higher security risks because of open data sharing.

Regarding the health and security of individuals, scientists obtain samples from people with the most severe disease for treatment failures. In this scenario, the risk includes the tendency to "underestimate the disease because most people don't get a sample, but you overestimate resistance because of the biases," as Dr. John Stelling, a medical doctor and co-director of the WHO collaborating center for surveillance of AMR, stated (interview, January 24, 2020). Additionally, the interviewee noted the risk of applying data directly from a treatment guideline where a doctor may incorrectly recommend a brand-new expensive drug when a cheaper drug would be more appropriate (interview, January 24, 2020). According to Dr. Stelling, "without an understanding of the data, without an understanding of the biases, you may incorrectly switch to new expensive drugs too early" (interview, January 24, 2020). Therefore, it is of paramount importance for the scientific and medical industry not wasting new agents but instead keeping the agents in reserve for possibly more significant threats in the circumstances such as the pandemic of COVID-19 and its variants.

Overseas production presents risks associated with international operations, which include volatile political and economic conditions, trade barriers, difficulties with training staff, unpredictable rates of exchanging foreign currency, and complex government regulations for foreign companies. Likewise, for a WHO medical officer, "the only risk is that we need to be transparent" (confidential telephone interview, Geneva, January 17, 2020). Committing to collaboration poses a risk to actors from diverse disciplines and social levels regarding balancing the scales of economic cost and collaborative benefits. Another concern is the risk of exposure to information in a global surveillance system, including whether the data are sufficiently anonymized to prevent identification of individuals or particular social groups.

Positive Outcomes: Challenges Posed by Collaboration, Interconnectedness, and Security Governance in New Pandemic Scenarios

A major challenge in studying network formation during a global health emergency or disaster entails identifying which actors collaborate and the link between the actors during a constantly disruptive setting. Analyzing interconnected actors is feasible in a centralized surveillance system such as the GLASS database and a known threat such as pathogens with AMR. Where there is a novel threat, such as the COVID-19 coronavirus, action to analyze collaboration is less feasible with heightened insecurity, misinformation, and fear of the unknown. In addition, where the research information originates from open sources or is publicly available information produced by organizations, creating a directed network does not make sense for a massive scale of constantly evolving information. Thus, analyzing collaboration and interconnection in security governance in the exchange of open-source information on the surveillance of infectious diseases makes better sense through an undirected network.

The challenge of collaboration in data sharing in an open source or publicly available information outlet brings challenges in accomplishing complicated tasks. For instance, "data vary considerably in terms of quality and completeness" (World Health Organization 2017b, 5). Complex problems of data access and privacy, both technological and on a policy level, remain a challenge on a cross-national domain level for regulatory and compliance environments. Technology regulations have become more important in the current context for different reasons. Technology regulations are migrating rapidly toward the virtual world for cultural, political, and social reasons. The role of digital platforms in society is not affected in the same way in all sectors of activity.

On the one hand, regulations reorganize economic, labor, and political participation toward a complete digital avenue that occurs rapidly in years to come. On the other hand, the issue of regulating freedom of expression and the mobilization of thought in social networks carries greater force in the context of a pandemic. For example, fake news on social networks and hacking of institutions to obtain vaccination research on the COVID-19 coronavirus increased during the COVID-19 pandemic. The regulation of technological infrastructure or ICTs in the virtual world are questions that have become more important than ever in contexts of pandemics, which set the stage for the governance of security matters for future threats.

Moreover, for intelligence analysts, in considering open source, care must be taken when reading the information in public domain. For instance, GLASS results provide limited information from the participating member-states. Furthermore, regional differences within a country are not reflected in aggregated data at the country level. Thus, the number of surveillance sites and isolates tested affects data reliability.

A trustworthy system of a health regime includes an interconnected global collaborative network to address global public health, such as the

GLASS case study. The challenge of having multiple actors from diverse fields coming together to tackle a global issue is like having many generals and only one soldier. The challenge presents the demand for time, amount of effort, and experts' contribution to participating in the surveillance process. Dr. Pablo Breuer noted: "I would like to think the decision-makers would call on experts" (interview, January 31, 2020). For instance, GLASS on AMR requires calling on doctors to figure out what information needs to be shared, lawyers to figure out the type of data that the customer cannot share, and security experts to advise on how to secure the data. At the end of the call, the project ends or stalls because a massive amount of information needs to be published immediately, or the stakeholders move forward without multiple expert collaborators. Dr. Pablo Breuer added that "it's always going to be a compromise, and the more interested parties that are in there, the more watered down the compromise has to be or tends to be" (interview, January 31, 2020). Therefore, disagreements exist within those groups even if all those experts come from one country and the decision-makers believe them. Thus, finding a middle ground assists in tackling the challenge.

Although collaboration poses many challenges, the magnitude of the COVID-19 challenge has shown the nation-states' political will to fix the problem of an outbreak, to rapidly get things done, and to unblock the barriers to progress. For example, efforts from diverse actors, including the private and public sectors, to support the development of vaccines during the COVID-19 pandemic illustrate international collaboration to eradicate the threat and recognize the importance of tackling an intrinsically global issue. However, some key challenges are misinformation, ill-informed policies, hesitancy in opting for a vaccine, and opposers.

Further challenges include "collecting robust surveillance data, particularly in countries with limited resources" (World Health Organization 2017b, 7). In addition, the analysis of massive amounts of information brings challenges, which include:

> [the] lack of standardized language found in datasets, the availability of technologies and computing power to support Big Data analytics, the security of the cyber infrastructure and data repositories, the privacy and

> confidentiality of individuals, and overfitting the analytic model to the data on which it was developed (American Association for the Advancement of Science, Federal Bureau of Investigation, and United Nations Interregional Crime and Justice Research Institute 2014, 9).

Moreover, a challenge is to think about security frameworks and how tech policies keep up with the rate of technology change around the world and to do so in a way that builds global frameworks. Likewise, an even more significant challenge to the worldwide health surveillance system is the initial reluctance to get involved. As with all new things, hesitation, confusion, or misinformation are impediments to the success of ideas and innovations. The same technologies or the intention to share information for the greater good is also a potential for destruction. The creators of the technology place their capabilities into the hands of diverse actors, whether human or nonhuman, increasing the chances for the system to crumble. However, we must consider the challenge of sharing too much information or letting people die. For this case study, the type of health regime and global surveillance system of common pathogens and its structure outweigh the challenge of having an overflow of information and the potential of the data to get into the wrong hands.

Another challenge is the binary categories we have developed to facilitate governance: the distinction between military and civilian, hard and soft power, external and internal, and peace and war. In addition, the line is increasingly blurred when dealing with multipurpose dual-use technologies. Finally, we need more multistakeholder engagement. Therefore, only some actors solve most of the challenges.

Vulnerabilities

This section touches upon the weakness or controversies in the system or application that malicious actors exploit. How do actors comprehend vulnerabilities regarding "unwanted intrusions and nefarious activities in the life science" (Murch et al. 2018, 2), as well as in cyberspace, to assist the intelligence community in identifying or responding to possible exploitations? The life sciences permeate the health, industrial, medical, food, and agricultural industries engaged in R&D on new medicines to deal with pandemics and the increasing number of infectious diseases. While actors are thus engaged in R&D, disruptions in the global supply chain of raw materials can affect the modern health care system. In addition, the actors are placing precautionary values in other areas, such as biosecurity, to mitigate the risk of science being used to harm humans, animals, plants, and the environment. This includes intentional releases of infectious disease agents, which can assist in detecting vulnerabilities in the system. Concomitantly, cybersecurity focuses on the "security of information technology-based systems, from personal computers and communications devices to large infrastructures and networks" (Murch et al. 2018, 2). A heightened awareness of the vulnerabilities and prioritizing the risks benefit customers such as stakeholders, high-level executives, boards of directors, clinicians, microbiologists, and workers engaged in controlling infections.

Vulnerability, at times, is "not clearly identifiable, often linked to a complex interdependence among related issues, and does not always suggest a correct or even adequate response" (Liotta 2002, 478-479). Nevertheless, vulnerability is "defined as an actor's liability to suffer costs imposed by external events even after policies have been altered" (Keohane and Nye 2012, 11). What policies deter other countries from exploiting vulnerabilities? What kinds of infrastructure and lessons to learn? There is a chance that the technology has some security risks, with an included cost of revamping or patching. As cyberbiological capabilities appear, coming together and sharing information help actors tackle global issues such as AMR and infectious diseases. Technologically advanced actors are compelled to think ahead, such as quantum computing, to avoid becoming offline.

Regarding human system vulnerabilities and data translation, "vulnerabilities . . . always have human dimensions" (Clark-Ginsberg, Abolhassani, and Rahmati 2018, 2). While the WHONET software development team applies the algorithms and tells the WHONET software what algorithms to run, issues of objective bias occur. For instance, Dr. John Stelling noted that if a scientist only tests an antibiotic such as imipenem on resistant strains, "you'll have an accurate number for the resistant strains, but not an accurate number for the population overall" (interview, January 24, 2020) which results in selective testing. Likewise, issues of selective sampling exist. Dr. Stelling also explained that in cases of urinary tract infections, a common infection in the microbiology laboratory affecting mainly women, only a few patients get a culture. In this scenario, many women take antibiotics independently and recover, and the scientists never get an adequate sample. Dr. Stelling indicated that out of a hundred women with urinary tract infections, "you'll often get five or ten samples and those tend to be the women with treatment failures, complicated medical histories, or recent discharge" (interview, January 24, 2020). Thus, the results turn out very biased, and human system vulnerabilities translate to a need for arriving at a more accurate interpretation. Therefore, such biases create vulnerabilities, overestimate resistance, and individuals create treatment guidelines based on biased information.

Likewise, vulnerabilities in the surveillance system include scientific controversies. For one interviewee, "the controversies are that you can't really assume that a universal set of conditions prevails and you have to get good information about the specific situatedness of the threat" (interview with Dr. Nancy Campbell, November 12, 2019). Similarly, for emerging and systematic vulnerabilities, AI systems are increasingly integrated in society and our daily lives from cell phones to health care technologies. As a game changer for every industry, AI is no longer the future, but the present. Regarding data security, as one interviewee remarked:

Colonel Patrick J. Mahaney Jr. As long as it's compliant with the established norms for cybersecurity which does change and includes periodic updates of software, anti-malware, and anti-viral software, then I think if we keep up with it as part of the standard regime, we are good to go (interview, February 14, 2020).

However, potentially complex new threats and vulnerabilities increase. Likewise, AI attacks represent a systematic and emerging vulnerability influencing the security of a country. Similarly, vulnerabilities in the data infrastructure and cyber ecosystem lead to inappropriate access to information. Therefore, the specifics-structural, political, and economic conditions-shape how, when, where, and to whom the threats manifest.

Other unwanted surveillance vulnerabilities exist in an emerging hybridized discipline, such as cyberbiosecurity at the intersection of cybersecurity and biosecurity, aimed at safeguarding bioeconomy. Some authors have defined cyberbiosecurity as:

> understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience (Murch et al. 2018, 1).

Other scholars define cyberbiosecurity as the intersection between biosafety procedures and cybersecurity (García Lirios 2021). A revised version of cyberbiosecurity encompasses "biological, medical and genomic information security vulnerabilities that arise from the interfacing of living and non-living systems, and the integration of living (animate) and non-living (inanimate) information substrates" (Dixon 2021, 688). In relation to the research conducted, actors utilize publicly available information to analyze and synthesize biological threats. As discussed earlier by the interviewees, it is difficult to weaponize common pathogens, including those monitored within the GLASS network. However, malicious actors have resorted to encoding malware into DNA sequences, which can compromise systems. The establishment of a trustworthy network such as GLASS plays a pivotal role in securing a health regime, providing an enriched global environment for research, development, and progress.

Nevertheless, cyberbiosecurity can protect "against threats resulting from the intricate relationships between computational and experimental workflow" (Peccoud et al. 2017, 4). Moreover, the biotechnology industry relies on nonhuman actors such as software, databases, and computer-controlled instruments to develop products. However, these vulnerable instruments present a potential target for cyberattacks. Therefore, it is neither prudent to remove technologies for fear of cyberattacks nor let the technology beast free without some security measures while keeping in mind the importance of now slowing down the process of innovation, data sharing, and production of health products. The risks of cyberbiosecurity entail, for instance, the interception of shipments which result in the injection of nefarious products that compromise a facility's operation, and the production of infectious agents due to corruption by altering sequences in a bioinformatics database (Peccoud et al. 2017). Although malicious actors slow down the progress of a network and science, the disruptor of the network allows us to understand the interconnection of the human and nonhuman dichotomy. Furthermore, the complex way multiple actors connect in GLASS allows us to understand the possible vulnerabilities that exist at a grander scale. For example, the research reveals that during data submission to the GLASS network in monitoring common bacterial pathogens that infect humans, the actors did not encounter malicious cyberattacks on the computer system. Every malevolent activity and every malicious actor require the actor network to innovate in order to strengthen collaboration.

In terms of finding the balance between cybersecurity, urgent security issues, the level of open data, and country data rights in the interest of national security, the study reveals that the more open actors create a database, the more data actors ingest, share, and collaborate. However, the more open the source becomes, the more vulnerable it is. Lieutenant Colonel Arnel P. David expressed the importance of taking security measures during information exchange and the value of privacy in the interest of national security and civil society: the interviewee noted that "you have to invest in the right security measures to ensure that people can't steal or manipulate the information" (interview, February 10, 2020). Thus, actors need to invest in the ability to collaborate equally.

Resources: Building Resilience Against Nontraditional Threats

During the initial impact of a global health emergency or disaster, many actors, including organizations and nation-states, come together to tackle the issue. In some instances, widespread illness leads to more severe disruption and forced interruptions that can prevent actors from communicating with one another and from sharing resources, leading actors to act autonomously. What efforts must be made across sectors to promote collaboration in creating and implementing technology? How do we ensure that it is done in a way that addresses concerns around global security, individual rights, and sustainable and equitable development? In other instances, global threats incentivize many actors to collaborate, pool their resources, and leverage their capacities. For example, a global system such as GLASS succeeds "through continued data sharing as well as global collaboration, harmonization, and coordination between partners" (World Health Organization 2017b, 6). Thus, through GLASS, the WHO creates a cross-border system that member-states use to report AMR data.

In the context of a health regime, resources include advice, support, accommodation, and work. Likewise, resources are "obtained in positive ways such as exploration, discovery, and trade or through negative means such as theft, murder, coercion, and fraud" (Omohundro 2019, 54). For instance, one party prevents another from doing something by withholding some resources. Nevertheless, resources, organizations, regulations, and statutes keep actors linked together (Latour 1999). In addition, "the drive to use resources efficiently seems to have primarily positive consequences" (Omohundro 2019, 54). Resources help inform decision-making, foster innovation, and support the global action plan on issues such as AMR.

Similarly, resources exist in a few concentrated areas, like knots of a mesh. Subsequently, connections to the knots or resources transform into a massive net extending in all directions (Latour 1987). Resources created from collaboration on AMR surveillance sometimes fail to perform but open the black box. The launch of GLASS moves toward the focus of an inquiry by other actors and organizations spreading across the leaves in the tree of resources. Therefore, the box is pried open even if a health regime is black-boxed in the surveillance process. Nation-states, institutions, researchers, scientists, and other actors use the content of GLASS reports for their interest and awareness.

For Dr. John Stelling, the virtual GLASS information is "useful for advocacy, gap identification, awareness, and fundraising" (interview January

24, 2020). Pooling resources builds resilience, connects knowledge across different fields, and enables the development of new methods, questions, and analysis. As another interviewee noted:

Colonel Patrick J. Mahaney Jr. It's a prima facie case to me as a realist that this type of cooperation is in our national interest, in the interest of our allies, friends, and consistent with our national values where we don't want people to die from diseases around the world. It doesn't help the world economy; it doesn't help the earth (interview, February 14, 2020).

Lieutenant Colonel Arnel P. David also remarked, "It's worth the risk of having this collaboration platform to collaborate than to not do it and risk not solving one of our world's human security challenges" (interview, February 10, 2020). Countries sharing their public-health surveillance data not only aid in identifying the sources of an outbreak, especially when it proves challenging at the national level, but also contributes to enhancing the capacity for detecting and responding to infectious diseases (Edelstein et al. 2018). Thus, collaborating with diverse actors enhances performance because of the greater pool of resources, matter, and accessible information to share, facilitating development.

On the one hand, nontraditional threats such as infectious diseases pose global challenges. On the other hand, these nonconventional threats also present opportunities within the collaborative network to respond better to threats and multipliers. At a macro level, "there is a need for understanding what the relative importance of all of these health issues is so that the government prioritizes actions and application of resources" (confidential telephone interview with a medical officer at the WHO, Geneva, February 26, 2020). Another interviewee noted:

Colonel Patrick J. Mahaney Jr. I think it's a great case of collaboration for common good that is consistent with our norms and values, laws of the United States, and the interests of the United States. It's another tool for national governments and alliances to enhance the security of their population whether it's their citizens or not. It's also a simple way to cooperate and to show collaboration in a positive way that does not cut down on your national sovereignty (interview, February 14, 2020).

Dr. Pablo Breuer remarked: "If we do it right, there's a tremendous benefit to information sharing and increasing knowledge in the medical community. But, still, there's also an enormous danger if we're not careful about how we do it" (interview, January 31, 2020).

Therefore, monitoring infectious diseases within a health regime creates security for individuals and nation-states, and the case study of the global AMR system of surveillance presents a perfect example of how international collaboration and cooperation arise, which significantly enhances concrete results both for the institution and nation-states.

Information exchange on an open database is necessary to counter nontraditional threats. Furthermore, information exchange improves the situational awareness of inherent nontraditional threats. The essential interaction of different actors, organizations, and disciplines increases a synergistic collaboration to mobilize resources. The interaction between various agents of continuity, such as the military, policymakers, teams handling medical emergencies, teams dealing with hazards, and intelligence experts increases situational awareness and real-time responses to reduce the impact of a strategic surprise. Thus, this cross-fertilization is an effective technique to counter nonconventional threats.

Moreover, through shared resources and capacity building, an urgent need arises for governments, institutions, and private-sector organizations to know more about how to keep their systems secure on a practical side, the type of data they transmit, and surveillance mechanisms for AMR pathogens. The GLASS network and further initiatives emerge globally to attempt to categorize all of the research on AMR and antibiotics to identify worldwide incidence. As a security effort, AMR surveillance ensures that researchers, scientists, shareholders, executives, leaders, and other actors do not reinvent the wheel and understand gaps. Resources, for instance, through the GLASS collaborative network, also assist in figuring out the investigatory nature of microbes and what kind of resources and the type of research are available. Ministries of health connect to government-to-government relations and work with global private-sector organizations. Therefore, the connections extend to understanding the methods of nation-states, responsibilities of institutions, what activities not to undertake, and which added activities and resources reinforce and strengthen practices.

This chapter analyzed security governance measures in the emergence of a health regime. Security governance is a crucial issue in health regimes, such as the one under study, because of the need to be globally connected and legally protected. However, as global threats increase, variables such as potential manipulation of human bias, blockages in information sharing and exchange, the lack of information, knowledge, and awareness, algorithmic mishaps, and cybercrimes challenge global health and security. The chapter shows how using various *dispositifs* and boundary objects, for instance, a technology system such as GLASS, policy instruments such as the IHR, and nonhuman actors such as infectious diseases, connects to a global surveillance system. Collectively, this study shows the necessity of actions by different actors to use resources such as open-source databases to balance the economic scales and tip the scales in favor of preparedness and response actions.

Obtaining and interpreting open data, and collaborating in response to a threat, present challenges because while everyone works together, many things that individuals work on are counterproductive. Nevertheless, information gathered through a collaborative effort of actors enables a better comprehension of the capacity to monitor infectious diseases and provides a mechanism for global reporting across nation-states. Regarding the equitable development and use of technology, the challenge lies in implementing and operationalizing norms. Likewise, technology is a curse and a blessing. On the one hand, innovations inspire creativity and, on the other hand, introduce new risks and dangers (Kurzweil 2019). The chapter also discussed the potential weaknesses in policy instruments. The International Health Regulations and international laws on cyberspace (United Nations Office for Disarmament Affairs 2021; World Health Organization 2016a) are a solid basis to start, and over time hope for more. However, the IHR developed norms and principles of behavior, and now is the time to drill down, analyze the details, and bring it down to a granular level. To be more systematic entails getting those at the front line, such as the private sector, civil society, academia, and the science sector. It also includes the private sector running the infrastructure to see new attacks emerging.

The COVID-19 pandemic highlighted the dynamic nature of malicious cyber operations, emphasizing the need for understanding the functioning of bias and the disruptive impact of cybercrimes on systems. To enhance the culture of the intelligence workflow, it is essential to integrate improved mobility, shorten the time to respond to a problem, and increase awareness. This can be achieved by incorporating a diverse range of experts, including auditors for scrutinizing bias, security teams for safety review, and data scientists for transparency. By reducing risks, modifying bias, and mitigating the negative effects of turnover, these experts contribute to a more resilient intelligence community culture (Clark 2020). Therefore, it is crucial to systematically engage diverse actors, not only in meetings or conferences, to drive the implementation of norms forward and leverage their expertise and practical experiences in utilizing technologies.

Chapter 5
Conclusions

> Only connect! That was the whole of her sermon.
> Only connect the prose and the passion, and both will be exalted, And human love will be seen at its height. Live in fragments no longer. Only connect …
>
> —E. M. Forster

The study's research design used a sequential explanatory strategy to map the network linking the nodes or agents, and also to learn about the collaborative performance of the actors and their interconnectedness. The mixed method is an intuitive research approach used in everyday life, multiple disciplines, and diverse industries. In this study, the method allowed the collection, combination, analysis, and integration of quantitative and qualitative data. Moreover, this mixed-method approach framed the procedure for the philosophical theories chosen for this study, and provided a complete understanding and explanation of the research problem.

The study integrated two separate analytical datasets, qualitative and quantitative, to transcend conventional statistical analysis and embrace a comprehensive and interconnected range of data. Gephi, a software package for statistical analysis of a network, was used for the creation of four network paths. Three tools were used for collecting data: semi-structured interviews, document analysis, and network analysis. This mixed-method approach to data collection yielded valuable insights by uncovering both commonalities and discrepancies across four distinct CNPs within different contextual scenarios. Additionally, a critical step in the process involved examining nodes with the highest degrees, a crucial aspect of network analysis, which helped in identifying the relevant details concerning the collaborative network. Understanding which actors held the highest degrees served as a valuable resource for enhancing or disrupting the connectivity and interdependence of the network. The pathways revealed the imperative of acknowledging the existence of collaborative networks within our complex and interdependent world.

This chapter is divided into four sections and synthesizes the study's contributions. The first section provides a summary of the findings. The second section examines the limitations throughout the investigation and offers various reflections on the study. The third section touches on the relevance of the study concerning the central research question. The fourth section provides potential ideas and recommendations to contribute to the literature on health, security, and science and technology studies. This section also includes final thoughts on global health issues, new security threats, and the involvement of technology.

Findings

Considering the intricacy of the topic at hand, this section provides further elaboration of the summary of findings and empirical chapters, delving into additional details. The analysis of this study revolves around the establishment and progression of a theoretical framework that encompasses three interrelated theories. By adopting this theoretical approach, the study unfolds through an exploration of three conceptual processes that have emerged in the field of international studies concerning health and security: complex interdependence, regimes, and security governance. Moreover, the research interconnects these theories and concepts by incorporating the notions of collaboration, boundary objects, *dispositifs*, and inscription devices, which serve as crucial bridging elements throughout the study.

The actor network theory captured the *dispositifs* that facilitated the inscription and translation process through the networks of human and nonhuman actors to break into objects. The study revealed, for instance, that the IHR, working as a *dispositif*, provided the rules to facilitate the process for participating member-states to act and collaborate in surveying infectious diseases. The GLASS database concerned common bacteria that have become resistant to antibiotics. As such, the bacteria became a menace, and the WHO declared AMR a global threat to public health. Motivated by the securitization theory, the study showed that the WHO raised the referent object to a higher level of threat on the political agenda. As a result, the IHR and the WHO cemented their value in security. The feeding of AMR information by member-states into GLASS as a venture of the WHO, in turn, manages and feeds the database networks. The examination of network expansion toward global South countries revealed their significant role in the surveying of pathogens and AMR. Acting as boundary objects, these actors serve as bridges between participating member-states and the submission process, facilitating effective exchange of information and collaboration in addressing these challenges. GLASS also assisted the inscription devices through the WHONET in producing and sharing data and monitoring bacterial pathogens that infect humans. In addition, the WHO assigned a designated priority to each pathogen based on the level of threat it posed, thereby establishing a protective measure of security against dangerous pathogens. Likewise, the internal WHO-GLASS officials reviewed the submitted AMR data before making the GLASS reports openly available. As a result, there was a level of data control and management, adding to the layers of security. A heightened awareness of global problems and new security threats based on technical data was presented through the interconnection of diverse actors and collaboration. Therefore, this study investigated a central topic regarding the connection between security and health through implementing and securitizing large databases and co-creating a security regime within a health regime.

The ANT assisted in expanding the understanding of actor dynamics within the network by integrating human and nonhuman actors, challenging the conventional boundaries of network analysis. This theoretical perspective provided deeper insights into the social processes and interactions between actors, reinforcing the liberal institutionalism theory, which highlights the vital role of nonstate actors. The study found that antimicrobial resistance (AMR) was a critical threat to human health, demanding global collaboration for effective containment strategies. Concurrently, during the research period, the emergence of the COVID-19 pandemic created unprecedented global challenges, leading to declarations of national emergencies and significant shifts in public-health priorities.

The pandemic illuminated critical limitations within the network. Industries worldwide, including research and development on AMR, came to a standstill, disrupting the ability of actors to input data into the system and hampering collaborative efforts. These challenges revealed the constraints imposed by external nonhuman actors, such as pandemics, and their capacity to hinder the effective functioning of networks. However, by 2021, renewed collaboration among diverse actors resulted in the establishment of a global antimicrobial resistance lab and response network, with numerous international partners collaborating across more than 38 countries.

These developments demonstrated how the actor-network theory facilitated an understanding of the complex interplay between internal dynamics and external influences within the network. The findings underscored that while the network faced significant obstacles, it also adapted to external pressures, highlighting the resilience and potential of collaborative frameworks. The ANT perspective further revealed that nonhuman actors, such as pandemics, were not only limitations but also catalysts for innovation and renewed global cooperation, driving progress in addressing both AMR and emerging health threats.

Under the liberal institutionalism theory, although the states maintained a primary role, other actors, such as institutions, also played a significant role in the surveillance of infectious diseases and AMR. Through the liberal institutionalism theory, the study showed how an institution such as the WHO and its GLASS architecture created peace-building mechanisms between participating countries to address common interests. The findings showed that the WHO pushed the boundaries for more collaborative actions by actors through its WHO AMR Surveillance and Quality Assessment Collaborating Centers Network, the regional surveillance networks, and the WHO regional offices. The liberal institutionalism theory emphasizes international organizations, global governance, and shared goals, such as surveillance of AMR or the fight against COVID-19. The results revealed that diverse actors, including states, participated in the collaborative network.

This research focused on the role of international organizations and the establishment of a health regime grounded in norms such as the IHR. The findings highlighted how the IHR facilitated security governance by structuring collaboration and addressing global health security challenges. These regulations connected nearly 200 countries, fostering international cooperation in public-health initiatives. The IHR served as a governing framework, promoting the interaction between nonstate and state actors to enhance the reporting and management of public-health emergencies, including AMR and emerging pandemics like COVID-19.

The study further revealed that countries participating in the IHR often engaged in parallel initiatives, such as the GLASS, enhancing collaborative efforts across platforms. The voluntary nature of participation within these frameworks demonstrated an increasing commitment to adhering to established regulations for monitoring communicable diseases. This collaboration reinforced the IHR's role in promoting a health regime by providing a structured and consistent set of rules to guide global health security efforts. Ultimately, the IHR proved instrumental in fostering a cohesive response to health threats, underscoring the importance of regulatory norms in managing complex interdependencies within the global health landscape.

Likewise, the securitization theory showed us the importance of referent objects and how actors tackle infectious diseases in pursuing the health and wellness of citizens and nations. The collaborative attribution of the GLASS data exchange in cyberspace revealed multiple nodes and edges (actors and links). The theory opened the door to the causal analysis of security governance in data and infectious diseases by reviewing the formality, efficiency, and material instruments through the operational, compliance, and technical metrics that added value to the global surveillance system. The findings showed that regulation of this space depended on the actors' level of responsibilities, the type of actions, and the different data sources. Thus, despite asymmetrical interests, operational measures enforce securitization considering the new existential threats and their future global influence.

The complex interdependence between network actors contributed to promoting a health regime by aligning efforts and harmonizing processes necessary for the effective sharing of substantial amounts of data. The case study of GLASS began with 42 participating countries in 2017, reflecting an initial wave of global collaboration. By 2020, the number of participating countries had risen to 96; and by 2021, it further increased to 109. However, disparities in participation were evident. For example, Brazil, an early participant, did not report AMR data during the initial years of its involvement. In October 2019, Argentina and Peru also joined the GLASS platform, but neither of these countries reported AMR data. These findings illustrate the uneven landscape of global collaboration, with certain countries encountering systemic or resource-based barriers that hinder their ability to fully contribute to the platform. Likewise, these findings highlight the uneven engagement across regions, emphasizing the need for further efforts to encourage broader and more consistent participation in global health surveillance systems.

Furthermore, by 2018, out of the major BRICS countries, Russia and India had become part of GLASS. During this period, China neither participated nor reported information into the GLASS database. The results revealed that gap-creating actors such as China and hackers appeared during the fieldwork research with different ties than those for the other network actors. The case study reinforced network analysis and showed the intricate formation of interconnected actor nodes. Therefore, the network analysis revealed the formation of interconnected clusters that encode indisputable complexity levels beyond a ternion.

The study found that both human and nonhuman actors interconnect in the security governance of infectious diseases to promote a health regime through mapping an ANT-inspired network that focuses on the heterogeneous networks of human and nonhuman actors to build collaboration and reinforce interconnectedness. The network mapping process involved using Gephi, a software application, which employs an algorithm that brings strongly connected actors closer together and pushes apart those with weaker connections. The network visualization revealed patterns and trends, highlighted outliers, and captured the story of interconnectedness and collaboration of actors.

Furthermore, this research extracted various statistical measures for network analysis, including connected components, clustering coefficient, density, degree, centrality, and modularity. The study's results showed that out of the four visualization path designs created during the quantitative data structure, the fourth network design, CNPD, presented the biggest network, which focused on the eight GLASS bacterial pathogens of human significance and the novel COVID-19 coronavirus infectious disease. The findings revealed that the GLASS pathogens, COVID-19, WHO, GLASS database, UN, IHR, and the WHA were the main actors in the network. Furthermore, private interest groups and NGOs, such as the Pew Charitable Trusts, leaned toward the middle of the interconnected collaborative network. Other actors, such as academic institutions including Columbia University (Mailman School of Public Health and School of International and Public Affairs) and the Rensselaer Polytechnic Institute, when incorporated into the network analysis, played minor roles in the GLASS network. Nonetheless, academic institutions contributed to advancing research, science, technology, and consultancy to the WHO on global health, AMR, and health and security.

Moreover, the degree of centrality illustrated the connections to all other actors in the network. The nodes with the highest betweenness centrality in different networks were as follows. CNPA: the WHO, GLASS database, GLASS pathogens, UN, and the IHR; CNPB: the WHO, GLASS pathogens, UN, IHR, and the WHA; CNPC: the WHO, UN, IHR, and the WHA; and CNPD: COVID-19, WHO, GLASS pathogens, GLASS database, and the UN. The investigation illustrated that these actors play significant roles in the collaboration and interconnectedness toward promoting a global health regime. Moreover, comparing all four network designs showed that the WHO and infectious diseases continue to lead as primary nodes for having high degrees and high betweenness centrality in connection to other nodes. The data showed that these actors are well-connected within clusters of the entire network.

Collectively, the CNPs showed the countries participating in GLASS as the most densely connected subgroup in the network. The findings revealed the average clustering coefficient with the respective network focal point: 0.416 clusters in the CNPA network (GLASS database and pathogens), 0.393 clusters in the CNPB network (GLASS database), 0.382

clusters in the CNPC network (GLASS pathogens), and 0.458 clusters in CNPD network (GLASS database, GLASS pathogens, and COVID-19). The low values of these coefficients showed that all other network actors are connected to the most significant weight nodes. The GLASS pathogens have low clusters because of their interconnection with the GLASS participating countries, who collaborate by submitting AMR surveillance information through their respective NCC into the GLASS platform.

The network's connected components show a common ideology amongst the actors, such as combating infectious diseases. Of the four networks, CNPA, CNPB, and CNPC had two weakly connected components whereas the CNPD network had five such components. Thus, a network's strong connection in becoming interconnected is based on the shared ideology of battling infectious diseases, sharing information to combat the threat, and increasing global health.

The network density reveals the number of actor ties divided by all possible network ties. At the same time, the node degree lists a node's connections to comparable nodes in the network. The density of network CNPA is 0.084, and the actors with the highest degrees are the WHO, GLASS database, GLASS pathogens, UN, and the IHR. The density of network CNPB is 0.068, and the actors with the highest degrees are the WHO, GLASS database, UN, IHR, and the WHA. The density of CNPC is 0.061, and the actors with the highest degrees are the WHO, GLASS pathogens, the UN, IHR, and the WHA. Lastly, the density of network CNPD is 0.043, and the actors with the highest degrees are the COVID-19, WHO, GLASS pathogens, GLASS database, and the UN. This network density reveals the nodes with the most significant number of connections in each of the networks. Thus, human and nonhuman actors play a vital role in network interconnectedness compared to nodes with fewer connections.

The research findings demonstrated the modular structure of each network path. The CNPA network comprised 117 nodes and exhibited a modularity of 0.050, divided into five distinct communities. Similarly, the CNPB network consisted of 119 nodes with a modularity of 0.054, also partitioned into five communities. The CNPC network, with 133 nodes, exhibited a modularity of 0.175 and was also divided into five communities. Lastly, the CNPD network consisted of 201 nodes and had a modularity of 0.256, organized into seven communities. Overall, the analysis demonstrated a clear segregation of networks into different communities, primarily centered around institutions, nonhuman actors, and countries.

The findings showed that although collaboration exists between nation-states at a macro level when there is a high degree of threat, additional actors such as institutions, funders, and private actors also contribute to data sharing and transparency. Meanwhile, at the meso level, actors such as security and intelligence, military and hazard teams, and data scientists and laboratories are paramount to knowledge production. Likewise, working with big data, algorithms, and intelligent technology also contributed to the dynamics of actors' human and nonhuman collaboration. Therefore, working in tandem with many different disciplines, diverse theories, and basic concepts delivers fruitful outcomes for communities and civil society. Sharing public-health surveillance data enables timely response and preparedness for global emergencies.

Limitations

In this section, a clear distinction is made between the limitations observed in the study and its practical application. Furthermore, additional reflections on the research are provided, offering deeper insights into the findings and their implications.

The case study on GLASS faces several limitations in obtaining data. First, it underscores that GLASS is in its early stages, starting data collection during the early implementation phase (2015-2019) and concluding the first data call in 2017. In many enrolled countries, GLASS encounters significant obstacles in obtaining reliable and representative data. In some countries, access to health care presents a notable challenge which impacts the reliability of data collection. This interplay between addressing AMR and health care underscores the importance of adequate coverage in facilitating both access and reliable testing, particularly in understanding the etiology of infections. Likewise, when a patient has a suspected infection, it can negatively interfere with the results. Therefore, the quality of microbiological tests which are performed could be more reliable. Besides, testing can be costly for countries, and strengthening laboratories in low- and mid-income countries is a challenge. Thus, the representation of data submitted to GLASS is limited, reflecting the challenges inherent in fostering a culture of surveillance to provide timely and accurate data.

Another limitation of the GLASS and its challenges with certain countries were remarked upon by an interviewee: "It's just tough to get the data that they need to make it a meaningful evaluation of what's going on. That's an ongoing challenge and it's probably not unique to antibiotic resistance data but they have their limitations" (confidential telephone interview with a PEW executive, United States, January 29, 2020).

Furthermore, other limitations are to develop comparative studies across different areas, such as the private sector, to draw broader conclusions about the role of networks in the surveillance of infectious diseases, data exchange in open-source access, and actor interconnectedness in health and security regime measures. What is required to work with and support the private sector and make progress in delivering the collaborative tools needed? Like COVID-19, how do we grapple with establishing suitable mechanisms to ensure that innovations are accessible to those who need them worldwide?

Moreover, while security reduces the possibility of data flowing freely, we know that, domestically and globally, political will is vital to making progress. Looking beyond the COVID-19 response, how do we reestablish that political will and gain fresh momentum in the response to AMR? Likewise, we need increased awareness of the complex and intricate processes involved in creating databases and reports, or their shared experience, as their creation depends on human effort. However, our minds and experiences condition our actions, so why not interconnect during the creation process into a kaleidoscope of elegant new opportunities?

Regarding the role of civil society and the general public, how will public attitudes toward global health issues such as AMR change in the post-pandemic era? Will we see more ambitious national and international efforts to fix global health problems? What else will we learn about the role of civil society organizations in mobilizing responses to significant health challenges on the frontline at the grassroots level? Preemptive measures to suppress a global pandemic require interconnection and collaboration from entities that include state and nonstate actors. Although nation-states maintain a primary role, it is not just one central actor but a combination of global actors, including NGOs, institutions, researchers, and academies, forming a worldwide collaborative network in the battle against infectious diseases.

In this section, a comprehensive overview is presented, highlighting the challenges and limitations encountered by researchers, data scientists, and intelligence analysts in their practice. Additionally, practical limitations in the field of surveillance and public policy are addressed. For instance, a specific limitation identified in the researcher's practice directly relates to conducting mixed-method research within the constraints of a 5-year doctoral program. To effectively carry out this type of research within the designated timeframe, it required a proactive and efficient approach from the very beginning of the academic program. The challenge was the need for a framework at the beginning of the program because the first year is usually dedicated to learning theories and concepts and attending full-time classes. Nevertheless, one thing is certain: to focus on qualitative data structure in conducting interviews. Interviews take a tremendous amount of time and energy, and sometimes interviewees may cancel interviews at the last minute. Therefore, a researcher needs to have patience and flexibility in the process of building the qualitative data structure. Thus, reaching out to potential interviewees early in the process is essential, as sometimes delays and sudden unexpected circumstances, such as a global pandemic, hinder the process of data collection.

Another limitation to improving mixed-method research involves researchers needing to look at outcomes and identify the shortcomings in practice, such as a lack of sufficient training and knowledge that can extend the time of a mixed-method research. For instance, it is valuable to the university or institute to offer the investigator appropriate training and resources to conduct a mixed-method study because projects or academic schedules have to be completed within the stipulated time. In turn, researchers rely on the university or institution to provide such training instead of wasting their time learning the skills using secondary sources such as YouTube because, it is assumed, that primary sources are better at teaching the mixed-method approach. YouTube, Google, or any other secondary sources are tools to supplement the training given by the institution. However, such supplementary training is a waste of time for researchers involved in a short program, and it would be more valuable to spend that time on the actual investigation.

On the other hand, suppose the institution lacks the resources to teach quantitative or mixed-method approach but is strong in social sciences or qualitative methodology, or vice versa. In that case, it may be better for the investigator to avoid the mixed-method approach. Therefore, there are limitations in the form of inadequate preparation for the mixed-method approach due to lack of time or training, which is likely to lead to obtaining results that fail to strike the right balance between qualitative and quantitative data.

Another limitation was that the fieldwork had to be during the COVID-19 pandemic, which made it difficult to enlist additional interviewees to encompass the remaining categories. At times, it took a great deal of effort to obtain further interviews, especially of high-level players, which entailed obtaining a security clearance. For instance, it took more than a year to schedule one interview alone at the WHO and to connect with the AMR department: initially, it was a virtual meeting mainly to build trust, and then it took one more year to conduct the actual interview, despite having complied with the requirement to submit the questionnaire beforehand. Time is of the essence in a doctoral program, and the unexpected global pandemic exacerbated the problem. Thus, unfortunately, researchers must work with what they have, which imposes limitations on their findings.

Despite the obstacles posed by the global pandemic, it was crucial to prioritize the quality of research over its quantity. In this particular study, recognizing the value of more time for a mixed-methods approach was essential. However, the limitations within the doctoral program's timeframe, combined with the challenges of the pandemic, affected the ability to connect and conduct interviews. Consequently, efforts were focused on securing interviews with highly regarded industry experts relevant to the single case study. Looking ahead, as borders gradually reopen and travel restrictions ease, future research endeavors can incorporate a wider range of interviewees from diverse fields and global actors in different countries. Similarly, in a post-pandemic context, having more time and greater flexibility in schedules may provide opportunities to conduct additional virtual interviews.

One limitation in the practice of a global surveillance system was that some countries need more infrastructure to submit information through laboratory work, more laboratory equipment, more sophisticated surveillance equipment, or appropriate transportation from the laboratory to the network. In addition, surveillance data "are not always freely shared because of perceived or real technical, political, economic, motivational, ethical, and legal barriers" (Edelstein et al. 2018, 1325). The GLASS network strove to allow countries to submit AMR data while understanding that not every country has the same robust information.

Likewise, essential infection control starts with surveillance to track down the spread both temporally and spatially and to determine the incubation period. Next, controlling the threat (virus) includes locating the source, isolation, or quarantine. Education is also paramount in the collaboration process, not just for the public but also for health care professionals and public-health officials to address and combat the threat. Finally, an institution creates a high level of legitimacy to gain trust in the system. Without such confidence, the participating countries would not include their information in a technology database to share data on bacterial pathogens of humans. Information governance to promote a health regime is built on trust in and legitimacy of the institution. However, in data sharing and information exchange through an open source, concerns of potential privacy issues are associated with the data. For example, although information exchange exists on platforms intended to be released publicly, problems arise regarding whether the data are used for good or bad purposes.

One limitation of public policy revealed during the study was identifed by an Ecuadorian medical doctor and microbiologist and temporary advisor to the PAHO, who explained that "obstacles arise because there are few doctors trained in infectious diseases, and you must educate. If you don't know something, you have to learn, because errors occur due to ignorance from lack of education" (Confidential telephone interview, Quito, February 25, 2022).

Therefore, for some South American countries, lack of adequate expertise in infectious diseases hinders their ability to submit appropriate and timely information on AMR to GLASS. The limitations of the study and in practice are situations that challenge actors such as decision-makers, stakeholders, researchers, and scientists working on achieving their objectives. However, these same challenges are learning curves and experiences as planning tools to improve operational efficiencies.

Relevance

This section explores the significance of the research in relation to the central research question and the theme, which examines the role of security governance in promoting a health regime through WHO's open-source intelligence technology for the surveillance of infectious diseases in the Americas from 2015 to 2021. The research sought to question whether the subject matter encompassing infectious diseases, health and security, and the incorporation of technology is a worthwhile contribution to the literature or merely a waste of space and time. In today's interconnected world, these topics have become increasingly intertwined and hold immense relevance, both within the realm of international studies and the domain of global health. Surveillance of infectious diseases and AMR remain at the forefront of regional and international agenda, contributing significantly to the knowledge base and informing health policies. Furthermore, our collective experience of the COVID-19 pandemic, its variants, and potential future health crises has underscored the paramount importance of a coordinated response, preparedness, and collaboration in addressing such challenges.

The findings of this study benefit various industries and stakeholders. For instance, the scale of global health, digital and interconnected security challenges, along with their corresponding preparedness and response strategies, exhibit parallels in context and dynamics. It is crucial to consider the diverse factors influencing these challenges in global health, security, and cybersecurity domains. In addition, sensibility includes stakeholders considering expectation management. At times, the idea of a panacea or a belief that one idea or a norm will solve all issues is a utopian ideology and is improbable: a dynamic process appears more probable. Addressing the challenges in these domains entails recognizing the complexity and fluidity of the issues instead of relying on a single solution or fixed approach, understanding the various factors, and adapting strategies as the situation evolves.

Similarly, the study highlights the significance of safety and security measures within the surveillance process, underscoring their crucial role in shaping the exchange of information and its impact on the international system. Furthermore, the research sheds light on the importance of collaborative networks and the disparities that exist among countries in terms of available resources and data strength. Consequently, the research offers valuable insights into the values and challenges at the intersection of health and security, showcasing the dynamics of two distinct worlds working together to foster a health regime. Moreover, it delves into how various actors use data to drive global health improvements, reflecting the transformative power of information in this context.

While the focus lies on global health and technology issues, other emerging technologies, such as AI, have entered the playing field. Moreover, AI uses its implements exponentially, which brings about new opportunities and challenges. Networks are a powerful tool to fill a gap in cybersecurity, which aligns assets, risks, and business. Networks assist in bridging the semantic gaps to make standard building blocks for detection systems. Reflecting on diverse theories and ontologies while looking at the different actors in the network, a concept such as community detection or modularity helps identify the densely connected nodes and analyze communities within the network. Depending on the theoretical perspective, network analysis and its concepts are valuable. For example, networks allow us to see the patterns of relations, and community detection is a helpful technique in machine learning to recognize groups with shared interests and properties. Thus, the key to addressing questions, opportunities, and challenges includes a collection of diverse actors and approaches from the bottom-up to top-down with mindfulness to obtain solutions cautiously.

Recommendations

This study offers new proposals, potential ideas, and recommendations in health, security, science, and technology since threats are all around us and will continue. In 2002, severe acute respiratory syndrome (SARS) appeared and quickly spread worldwide. In 2009, the H1N1 influenza pandemic emerged. In 2013, we had the West Africa Ebola outbreak. Some of the same issues during these epidemics appeared during the COVID-19 pandemic. Over the past 20 years, significant regional and global infectious diseases have spread over wider areas. What lessons do we learn from these recent pandemics to help us deal with the next known or unknown pandemic? Public-health planners, strategists, researchers, and security and intelligence analysts must test public-health policies before implementing them. How do we succeed now and in the future? Listening to public-health and security experts contributes to the solution. Experts continue to work on refining problems but also need political leadership to make the deals that close the gaps. For example, we need to be better at taking advantage of sharing health care data or information from AMR surveillance provided through collaboration among scientists. Thus, placing science and health security experts at the forefront of the level of governance is essential.

Furthermore, a multitude of information is being dispersed. However, information needs to be communicated to the public to make it meaningful. Hence, there is less division and more comprehension to help protect the public and reduce the risk of exposure. During the pandemic, it is paramount to see greater power collaboration and interconnectedness and less power competition. Viruses are invisible and transcend national borders. The asymptomatic nature of many viruses also challenges the public-health system. In order to prepare for the next outbreak, it is valuable to look at platform technologies–whether diagnostics, developing new vaccines, or managing security issues–that enable us to respond rapidly to a range of different types of threats. Investing in international collaboration is essential. Bringing scientists, security, intelligence, military, and legal experts from different countries together will help to communicate during a crisis. There must be a combination of different entities, not just NGOs or funders. For instance, a collaboration of diverse actors shares and disseminates information as widely as possible to make the best-informed decision on the actual risks. Another suggestion for greater intelligence is the actors' appreciation of the contribution of each actor to the network and the value of open exchange of information, which influences the continuity of collaborative interconnection. Therefore, we need to improve multistakeholder integration and more meaningful engagement.

Likewise, in context and dynamics, preparedness and response are paramount to match the magnitude of global health, digital technologies, and interconnected security challenges. In addition, expectation management is vital for stakeholders to consider. Managing the expectations in addressing a global health concern includes open and transparent communication, in simple rather than technical terms, so that all parties involved clearly understand what to expect from the process. Therefore, open communication makes the process of collaboration more promising.

By acknowledging the interconnectedness of health and security, we can foster a more comprehensive approach to addressing threats and vulnerabilities. This entails prioritizing public-health preparedness, investing in robust surveillance and response systems, and integrating health considerations into national security strategies. Economic awareness is paramount in understanding that escalating and diversifying mean a substantial investment in innovation, research, and development in response to the threat of infectious diseases and AMR affecting all countries. These ideas enhance the support of the global action plan on AMR in the fight to combat emerging threats, help informed decision-making, and harmonize action for human, animal, plant, and global environmental health.

To foster interconnection and collaboration among research institutions and governments, the recommendation is to establish an immersive network that transcends specific agencies, spanning multiple organizations and sectors. A network of actors that tackles alternative security measures while operating within the context of open source or radical transparency is feasible. For example, adaptable data security measures include advanced management systems or sources of access control instead of relying on traditional encryption methods and creating a trusting network by increasing communication and transparency. The latter assists in identifying malicious actors and decreasing possible threats. A collaborative union is pertinent to dissipate the threat in a world full of corruption, power-mongering, and greed, where nation-states face enormous national security challenges such as global infectious diseases. Interconnectedness (or network analysis) broadens partnerships, builds diplomatic relationships, and brings awareness of the potential repercussions of security breaches when multiple collaborative measures exist.

Networks open the lens of existing problems to promote a health regime in security governance and surveillance of infectious diseases through open-source intelligence or publicly available information. In addition, norms are valuable in de-escalating issues such as spreading false public-health information, addressing existing and future threats, and mitigating security risks in the health care space created by malevolent actors and data attacks.

In conclusion, the specific case study delved into the following research question: Why did security governance through a WHO open-source intelligence technology database promote the health regime on the surveillance of infectious diseases in the Americas from 2015 to 2021? The study successfully validated the hypothesis, indicating that security governance is instrumental in establishing a contemporary health regime to effectively address unconventional threats. Additionally, it is important to reiterate the three objectives outlined in the introductory chapter, which served as the guiding principles throughout this study. First, the study opened the black box of a health regime by examining the open exchange of data within GLASS and its role in monitoring infectious diseases. Secondly, the study analyzed the development of a health regime by showcasing the emergence of unconventional threats that triggered the activation of security governance through collaborative dynamics, *dispositifs*, and boundary objects in the context of open information exchange. Thirdly, the research provided an explanation for the significance of security governance in securing a health regime during the open exchange of *ingentis* data, addressing associated risks, vulnerabilities, and available resources within the utilization of GLASS for the construction of a health regime in the surveillance of communicable diseases.

As this research concludes, it becomes evident that sustainable changes in workflow and a willingness to adapt are necessary to foster a health regime capable of effectively monitoring infectious diseases while tackling secondary nonconventional threats. It is crucial to think innovatively and leverage the global structure of GLASS as a foundation for promoting collaboration among actors on a larger scale to tackle global issues. This approach allows us to grasp the potential of interconnectedness in dealing with complex challenges within our interdependent world.

References

Abbassi, Zeinab, and Vahab S. Mirrokni. 2007. "A Recommender System Based on Local Random Walks and Spectral Methods." *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining and Social Network Analysis*. New York, NY: ACM. https://doi.org/10.1145/1348549.1348561.

Abbott, Kenneth W., and Duncan Snidal. 1998. "Why States Act through Formal International Organizations." *The Journal of Conflict Resolution* 42 (1): 3–32. http://www.jstor.org/stable/174551

Adler, Emanuel, and Patricia Greve. 2009. "When Security Community Meets Balance of Power: Overlapping Regional Mechanisms of Security Governance." *Review of International Studies* 35 (S1): 59–84. https://doi.org/10.1017/S0260210509008432

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. 2020. "La Estrategia Digital Frente al Coronavirus COVID-19." https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/estrategia-digital-frente-coronavirus-covid-19

Aggarwal, Mayank, Anindya S. Chakrabarti, Chirantan Chatterjee, and Matthew J. Higgins. 2023. "Research and Market Structure: Evidence from an Antibiotic-Resistant Pathogenic Outbreak." *Research Policy* 52 (1): 104633. https://doi.org/10.1016/j.respol.2022.104633

Akrich, Madeleine. 1992. "The De-Scription of Technical Objects." In *Shaping Technology- Building Society: Studies in Sociotechnical Change*, edited by Wiebe E. Bijker and John Law, 205–24. Cambridge, MA: The MIT Press. https://hdl.handle.net/2027/heb01128.0001.001

Akrich, Madeleine, and Cécile Méadel. 2012. "Policing Exchanges as Self-Description in Internet Groups." In *Governance, Regulation and Powers on the Internet*, edited by Eric Brousseau, Meryem Marzouki, and Cécile Méadel, 232–56. Cambridge: Cambridge University Press. https://doi.org/DOI:10.1017/CBO9781139004145.015

Albornoz, María Belén. 2020. *Habitar las redes: las controversias sobre la privacidad en Facebook*. Quito: FLACSO Ecuador. https://doi.org/10.46546/20209atrio

Albornoz, María Belén, Mónica Bustamante Salamanca, and Javier Jiménez Becerra. 2013. *Computadores y cajas negras*. Quito: FLACSO. https://biblio.flacsoandes.edu.ec/libros/131285-opac

American Association for the Advancement of Science, Federal Bureau of Investigation, and United Nations Interregional Crime and Justice Research Institute. 2014. "National and Transnational Security Implications of Big Data in the Life Sciences." Washington, DC. https://www.aaas.org/sites/default/files/AAAS-FBI-UNICRI_Big_Data_Report_111014.pdf

Antibiotics Research Institute, Huashan Hospital Affiliated to Fudan University. 2021. "CHINET: China Bacterial Resistance Surveillance Network (in Chinese)." https://www.chinets.com

Anzivino, Nicola, Paolo Anfossi, and Dario Saracino. 2021. "Artificial Intelligence Evolution: Main Trends." PricewaterhouseCoopers. March 18. https://web.archive.org/web/20240210190021/https://www.pwc.com/it/it/publications/assets/docs/pwc-ai-evolution-financial-services.pdf

Arvanitis, Rigas. 2009. "Science and Technology Policy." In *Science and Technology Policy: Encyclopedia of Life Support Systems*, edited by Rigas Arvanitis, 1-61. Oxford: Eolss Publishers.

Ashley, Elizabeth A., Nandini Shetty, Jean Patel, Rogier van Doorn, Direk Limmathurotsakul, Nicholas A Feasey, Iruka N. Okeke, and Sharon J. Peacock. 2019. "Harnessing Alternative Sources of Antimicrobial Resistance Data to Support Surveillance in Low-Resource Settings." *Journal of Antimicrobial Chemotherapy* 74 (3): 541–46. https://doi.org/10.1093/jac/dky487

ASPE (Office of The Assistant Secretary for Planning and Evaluation). 2020. "National Action Plan for Combating Antibiotic-Resistant Bacteria, 2020-2025." October 8. https://aspe.hhs.gov/reports/national-action-plan-combating-antibiotic-resistant-bacteria-2020-2025

Balzacq, Thierry. 2010. *Securitization Theory*. Edited by Thierry Balzacq. Routledge. https://doi.org/10.4324/9780203868508

— 2015. "The 'Essence' of Securitization: Theory, Ideal Type, and a Sociological Science of Security." *International Relations* 29 (1): 103–13. https://doi.org/10.1177/0047117814526606b

Balzacq, Thierry, and Myriam Dunn Cavelty. 2016. "A Theory of Actor-Network for Cyber-Security." *European Journal of International Security* 1 (2): 176–98. https://doi.org/10.1017/eis.2016.8

Banks, Michael. 1985. "The Inter-Paradigm Debate." In *International Relations: A Handbook on Current Theory*, edited by A.J.R. Groom and Margo Light, 7–26. London: Pinter Publishers.

Barnes, John A. 1979. "Network Analysis: Orienting Notion, Rigorous Technique or Substantive Field of Study?" In *Perspectives on Social Network Research*, edited by Paul W. Holland and Samuel Leinhardt, 403–23. Elsevier. https://doi.org/10.1016/B978-0-12-352550-5.50024-9

Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy. 2009. "Gephi: An Open Source Software for Exploring and Manipulating Networks." *Proceedings of the International AAAI Conference on Web and Social Media* 3 (1): 361–62. https://doi.org/10.1609/icwsm.v3i1.13937

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: SAGE.

Berthod, Olivier, Michael Grothe-Hammer, Gordon Müller-Seitz, Jörg Raab, and Jörg Sydow. 2016. "From High-Reliability Organizations to High-Reliability Networks: The Dynamics of Network Governance in the Face of Emergency." *Journal of Public Administration Research and Theory*, September. https://doi.org/10.1093/jopart/muw050

Bevir, Mark. 2007. *Encyclopedia of Governance*. Thousand Oaks, CA: SAGE. https://doi.org/10.4135/9781412952613

Blanton, Shannon L., and Charles W. Kegley. 2017. *World Politics: Trends and Transformation*. Boston, MA: Cengage Learning.

Blondel, Vincent D., Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre. 2008. "Fast Unfolding of Communities in Large Networks." *Journal of Statistical Mechanics: Theory and Experiment* 2008 (10): P10008. https://doi.org/10.1088/1742-5468/2008/10/P10008

Borgatti, Stephen P., Martin G. Everett, and Jeffrey C. Johnson. 2013. *Analyzing Social Networks*. London: SAGE.

Boudia, Soraya. 2014. "Managing Scientific and Political Uncertainty: Environmental Risk Assessment in a Historical Perspective." In *Powerless Science?: Science and Politics in a Toxic World*, edited by Soraya Boudia and Nathalie Jas, 95–112. Berghahn Books. https://doi.org/10.2307/j.ctt9qd0tj.9

Bowker, Geoffrey C. 2000. "Biodiversity Datadiversity." *Social Studies of Science* 30 (5): 643–83. https://doi.org/10.1177/030631200030005001

— 2001. "The New Knowledge Economy and Science and Technology Policy." In *Science and Technology Policy: Encyclopedia of Life Support Systems*, edited by Rigas Arvanitis, 285-303. Oxford: Eolss Publishers.

— 2006. *Memory Practices in the Sciences*. Cambridge, MA: The MIT Press.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out*. Cambridge, MA: The MIT Press. https://doi.org/10.7551/mitpress/6352.001.0001

Brady, Mark F., Zohaib Jamal, and Najwa Pervin. 2021. "Acinetobacter." In *StatPearls [Internet]*. Treasure Island, FL: StatPearls Publishing.

Breakspear, Alan. 2013. "A New Definition of Intelligence." *Intelligence and National Security* 28 (5): 678–93. https://doi.org/10.1080/02684527.2012.699285

Brousseau, Eric, Meryem Marzouki, and Cécile Méadel. 2012. "Governance, Networks and Digital Technologies: Societal, Political and Organizational Innovations." In *Governance, Regulation and Powers on the Internet*, edited by Eric Brousseau, Meryem Marzouki, and Cécile Méadel, 3–36. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139004145.002

Brower, Jennifer, and Peter Chalk. 2003. *The Global Threat of New and Reemerging Infectious Diseases: Reconciling U.S. National Security and Public Health Policy*. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/MR1602.

Buckley, Chris, and Steven Lee Myers. 2020. "As New Coronavirus Spread, China's Old Habits Delayed Fight." The New York Times, February 1. https://www.nytimes.com/2020/02/01/world/asia/china-coronavirus.html.

Bull, Hedley. 1977. *The Anarchical Society*. London: Macmillan Education UK. https://doi.org/10.1007/978-1-349-24028-9.

Buzan, Barry, and Richard Little. 2000. *International Systems in World History: Remaking the Study of International Relations*. Oxford University Press.

Buzan, Barry, and Ole Wæver. 2003. *Regions and Powers*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511491252.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner.

Callon, Michel, John Law, and Arie Rip, eds. 1986. *Mapping the Dynamics of Science and Technology*. London: Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-07408-2.

Carril, Enrique del. 2020. "El Estado como garante de seguridad del ciudadano individual. Desafíos vinculados con el cibercrimen y el ciberdelito. Desafíos normativos y ejecutivos." In *Desafíos de la administración pública en el contexto de la revolución 4.0*, edited by Santiago Bellomo and Oscar Oszlak, 61–84. Ciudad Autónoma de Buenos Aires: Konrad Adenauer Stiftung.

CDC. 2019a. "Antibiotic Resistance Threats in the United States, 2019." Atlanta, GA. https://doi.org/10.15620/cdc:82532.

— 2019b. "MRSA General Information." U.S. Centers for Disease Control and Prevention. August 21. https://www.cdc.gov/mrsa/community/index.html.

— 2022. "COVID-19: U.S. Impact on Antimicrobial Resistance, Special Report 2022." Atlanta, GA. https://www.cdc.gov/antimicrobial-resistance/media/pdfs/covid19-impact-report-508.pdf.

Cecchine, Gary, and Melinda Moore. 2006. *Infectious Disease and National Security: Strategic Information Needs*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/technical_reports/TR405.html.

Chen, Lincoln, and Vasant Narasimhan. 2003. "Human Security and Global Health." *Journal of Human Development* 4 (2): 181–90. https://doi.org/10.1080/1464988032000087532.

Chorev, Nitsan. 2012. *The World Health Organization between North and South*. Ithaca and London: Cornell University Press. https://www.cornellpress.cornell.edu/book/9780801450655/the-world-health-organization-between-north-and-south.

CISA (Cybersecurity and Infrastructure Security Agency), and ACSC (Australian Cyber Security Centre). 2022. "2021 Top Malware Strains." https://www.cisa.gov/sites/default/files/publications/aa22-216a-2021-top-malware-strains.pdf.

Clark, Robert M. 2020. *Intelligence Analysis. A Target-Centric Approach*. Washington, DC: CQ Press. https://collegepublishing.sagepub.com/products/intelligence-analysis-7-274957.

Clark-Ginsberg, Aaron. 2017. "Participatory Risk Network Analysis: A Tool for Disaster Reduction Practitioners." *International Journal of Disaster Risk Reduction* 21 (March): 430–37. https://doi.org/10.1016/j.ijdrr.2017.01.006.

— 2020. "Disaster Risk Reduction Is Not 'Everyone's Business': Evidence from Three Countries." *International Journal of Disaster Risk Reduction* 43 (February): 101375. https://doi.org/10.1016/j.ijdrr.2019.101375.

Clark-Ginsberg, Aaron, Leili Abolhassani, and Elahe Azam Rahmati. 2018. "Comparing Networked and Linear Risk Assessments: From Theory to Evidence." *International Journal of Disaster Risk Reduction* 30 (September): 216–24. https://doi.org/10.1016/j.ijdrr.2018.04.031.

Claude, Inis L. 1971. *Swords Into Plowshares: The Problems and Progress of International Organization*. New York, NY: Random House.

Coate, Roger A., Jeffrey A. Griffin, and Steven Elliott-Gower. 2015. "Interdependence in International Organization and Global Governance." In *Oxford Research Encyclopedia of International Studies*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190846626.013.110.

Congress.gov. 2018. "Congress.GovH.R.5356 - 115th Congress (2017-2018): To Establish the National Security Commission on Artificial Intelligence." May 22, 2018. https://www.congress.gov/bill/115th-congress/house-bill/5356.

Cox, Robert W., and Harold K. Jacobson. 1973. *The Anatomy of Influence: Decision Making in International Organizations*. New Haven and London: Yale University Press.

Creswell, John. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Thousand Oaks, CA: SAGE.

Creswell, John, and Vicki L. Plano. 2018. *Designing and Conducting Mixed Methods Research*. Thousand Oaks, CA: SAGE.

Danks, David, and Alex John London. 2017. "Algorithmic Bias in Autonomous Systems." In *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, 4691–97*. California City, CA: International Joint Conferences on Artificial Intelligence Organization. https://doi.org/10.24963/ijcai.2017/654.

David, Paul A. 1985. "Clio and the Economics of QWERTY." *The American Economic Review* 75 (2): 332–37. http://www.jstor.org/stable/1805621.

de Groot, Raoul J., Susan C. Baker, Ralph S. Baric, Caroline S. Brown, Christian Drosten, Luis Enjuanes, Ron A. M. Fouchier, Monica Galiano, Alexander E. Gorbalenya, Ziad A. Memish, Stanley Perlman, Leo L. M. Poon, Eric J. Snijder, Gwen M. Stephens, Patrick C. Y. Woo, Ali M. Zaki, Maria Zambon, and John Ziebuhr. 2013. "Commentary: Middle East Respiratory Syndrome Coronavirus (MERS-CoV): Announcement of the Coronavirus Study Group." *Journal of Virology* 87 (14): 7790–92. https://doi.org/10.1128/JVI.01244-13.

Denzin, Norman, and Yvonna Lincoln, eds. 2008. *The Landscape of Qualitative Research*. 3rd ed. SAGE.

Dion, Christopher F., and John V. Ashurst. 2021. "Streptococcus Pneumoniae." In *StatPearls [Internet]*. Treasure Island, FL: StatPearls Publishing.

D'Israeli, Isaac. 1807. *Curiosities of Literature*. Edited by The Earl of Beaconsfield. Vol. 1. London: Frederick Warne and Co.

Dixon, Thom. 2021. "The Grey Zone of Cyber-Biological Security." *International Affairs* 97 (3): 685–702. https://doi.org/10.1093/ia/iiab041.

Dryzek, John S. 2009. "Policy Analysis as Critique." In *The Oxford Handbook of Public Policy*, edited by Robert E. Goodin, Michael Moran, and Martin Rein, 190–204. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199548453.003.0009.

Edelstein, Michael, Lisa M. Lee, Asha Herten-Crabb, David L. Heymann, and David R. Harper. 2018. "Strengthening Global Public Health Surveillance through Data and Benefit Sharing." *Emerging Infectious Diseases* 24 (7): 1324–30. https://doi.org/10.3201/eid2407.151830.

Einstein, Albert. 2011. *Out of My Later Years*. New York, NY: Open Road Integrated Media. https://openroadmedia.com/ebook/out-of-my-later-years/9781453204894.

Eroukhmanoff, Clara. 2017. "Securitisation Theory." In *International Relations Theory*, edited by Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug. Bristol: E-International Relations.

Executive Office of the President. 2020. "Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak." Federal Register. March 13. https://www.federalregister.gov/d/2020-05794.

— 2021. "Continuation of the National Emergency Concerning the Coronavirus Disease 2019 (COVID-19) Pandemic." Federal Register. February 26, 2021. https://www.federalregister.gov/d/2021-04173.

FAO (Food and Agriculture Organization of The United Nations). 2018. *Assessing The Contribution of Bioeconomy to Countries' Economy. A Brief Review of National Frameworks*. https://www.fao.org/3/I9580EN/i9580en.pdf.

FEMA (Federal Emergency Management Agency). 2020. "COVID-19 Emergency Declaration." March 14. https://www.fema.gov/press-release/20250121/covid-19-emergency-declaration.

Feng, Shihui, and Alec Kirkley. 2020. "Mixing Patterns in Interdisciplinary Co-Authorship Networks at Multiple Scales." *Scientific Reports* 10 (1): 7731. https://doi.org/10.1038/s41598-020-64351-3.

Fidler, David P. 2003. "Public Health and National Security in the Global Age: Infectious Diseases, Bioterrorism, and Realpolitik Diseases, Bioterrorism, and Realpolitik." *George Washington International Law Review* 787. https://www.repository.law.indiana.edu/facpub/416.

Figge, Helen. 2018. "Deploying Artificial Intelligence against Infectious Diseases." *US Pharm* 43 (3): 21–24. https://www.qgdigitalpublishing.com/publication/?i=479929&p=42&view=issueViewer.

Fontaine, Guillaume. 2016. *El Análisis de Políticas Públicas. Conceptos, Teorías y Métodos*. Barcelona: Anthropos Editorial / FLACSO Ecuador.

Foucault, Michel. 1980. "The Confession of the Flesh." In *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*, edited by Colin Gordon. New York: Pantheon Books.

Frank, Aaron Benjamin, Margaret Goud Collins, Simon A. Levin, Andrew W. Lo, Joshua Ramo, Ulf Dieckmann, Victor Kremenyuk, Arkady Kryazhimskiy, JoAnne Linnerooth-Bayer, Ben Ramalingam, J. Stapleton Roy, Donald G. Saari, Stefan Thurner, and Detlof von Winterfeldt. 2014. "Dealing with Femtorisks in International Relations." *Proceedings of the National Academy of Sciences* 111 (49): 17356–62. https://doi.org/10.1073/pnas.1400229111.

Frank, Eibe, Mark A. Hall, and Ian H. Witten. 2016. *The WEKA Workbench. Online Appendix for Data Mining: Practical Machine Learning Tools and Techniques*. Edited by Morgan Kaufman. https://www.cs.waikato.ac.nz/ml/weka/Witten_et_al_2016_appendix.pdf.

Fulmer, Russell. 2019. "Artificial Intelligence and Counseling: Four Levels of Implementation." *Theory & Psychology* 29 (6): 807–19. https://doi.org/10.1177/0959354319853045.

G20 Riyadh Summit. 2020. "Leaders' Declaration." 2020. https://g20.org/summit-and-logos/2020-riyadh/.

G20 Saudi Arabia 2020. 2020. "Extraordinary G20 Leaders' Summit. Statement on COVID-19." https://www.consilium.europa.eu/media/43072/final-g20-leaders-statement-26032020.pdf.

Gaillard, Jacques, and Rigas Arvanitis, eds. 2013. *Research Collaboration between Europe and Latin America. Mapping and Understanding Partnership*. Paris: Éditions des archives contemporaines. https://eac.ac/publications/9782813001245.

García Lirios, Cruz. 2021. "Bioseguridad y ciberseguridad percibidas ante la COVID-19 en México." *Estudios en Seguridad y Defensa* 16 (31): 137–60. https://doi.org/10.25062/1900-8325.293.

Gaudillière, Jean-Paul. 2014. "DES, Cancer, and Endocrine Disruptors: Ways of Regulating, Chemical Risks, and Public Expertise in the United States" In *Powerless Science? Science and Politics in a Toxic World*, edited by Soraya Boudia and Nathalie Jas, 65–94. Berghahn Books. https://doi.org/10.2307/j.ctt9qd0tj.8.

Ghebreyesus, Tedros Adhanom. 2018. "Artificial Intelligence for Good Global Summit." World Health Organization. May 15. https://www.who.int/director-general/speeches/detail/artificial-intelligence-for-good-global-summit.

Gibert, Daniel, Carles Mateu, and Jordi Planes. 2020. "The Rise of Machine Learning for Detection and Classification of Malware: Research Developments, Trends and Challenges." *Journal of Network and Computer Applications* 153 (March): 102526. https://doi.org/10.1016/j.jnca.2019.102526.

Gieryn, Thomas F. 1983. "Boundary-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideologies of Scientists." *American Sociological Review* 48 (6): 781. https://doi.org/10.2307/2095325.

Glauser, Wendy. 2018. "Blood-Delivering Drones Saving Lives in Africa and Maybe Soon in Canada." *Canadian Medical Association Journal* 190 (3): E88–89. https://doi.org/10.1503/cmaj.109-5541.

Gobernación de la Provincia de Loja. 2020. "Presentación Oficial de La Aplicación Digital 'ASÍ Ecuador' En Loja." August 18. https://gobernacionloja.gob.ec/wp-content/uploads/downloads/2020/agosto/boletines.pdf.

Goffman, Erving. 1956. *The Presentation of Self in Everyday Life*. Edinburgh: University of Edinburgh.

Goldman, Michael. 2005. *Imperial Nature. The World Bank and Struggles for Social Justice in the Age of Globalization*. Yale University Press.

Grieco, Joseph M. 1988. "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism." *International Organization* 42 (3): 485–507. https://doi.org/10.1017/S0020818300027715.

Grix, Jonathan. 2002. "Introducing Students to the Generic Terminology of Social Research." *Politics* 22 (3): 175–86. https://doi.org/10.1111/1467-9256.00173.

Grotius, Hugo. 1901. *The Rights of War and Peace*. New York & London: M. Walter Dunne. https://oll.libertyfund.org/titles/grotius-the-rights-of-war-and-peace-1901-ed.

Guzzini, Stefano. 2011. "Securitization as a Causal Mechanism." *Security Dialogue* 42 (4/5): 329–41. http://www.jstor.org/stable/26301792.

Haas, Ernst B. 1975. "Is There a Hole in the Whole? Knowledge, Technology, Interdependence, and the Construction of International Regimes." *International Organization* 29 (3): 827–76. https://doi.org/10.1017/S0020818300031787.

— 1980. "Why Collaborate? Issue-Linkage and International Regimes." *World Politics* 32 (3): 357–405. https://doi.org/10.2307/2010109.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organization* 63 (3): 559–92. https://doi.org/10.1017/S0020818309090195.

Halford, Susan, and Mike Savage. 2017. "Speaking Sociologically with Big Data: Symphonic Social Science and the Future for Big Data Research." *Sociology* 51 (6): 1132–48. https://doi.org/10.1177/0038038517698639.

Hall, Mark, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. 2009. "The WEKA Data Mining Software." *ACM SIGKDD Explorations Newsletter* 11 (1): 10–18. https://doi.org/10.1145/1656274.1656278.

Henderson, Donald A. 1993. "Surveillance Systems and Intergovernmental Cooperation." In *Emerging Viruses*, edited by Stephen S. Morse, 283–89. Oxford University Press. https://doi.org/10.1093/oso/9780195074444.003.0027.

Hendrickson, Noel. 2008. "Critical Thinking in Intelligence Analysis." *International Journal of Intelligence and CounterIntelligence* 21 (4): 679–93. https://doi.org/10.1080/08850600802254749.

Hernández, Javier C., and James Gorman. 2021. "On W.H.O. Trip, China Refused to Hand Over Important Data." February 12. https://www.nytimes.com/2021/02/12/world/asia/china-world-health-organization-coronavirus.html.

Hesse-Biber, Sharlene Nagy. 2015. "Introduction: Navigating a Turbulent Research Landscape: Working the Boundaries, Tensions, Diversity, and Contradictions of Multimethod and Mixed Methods Inquiry." In *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*, edited by Sharlene Nagy Hesse-Biber and R. Burke Johnson, xxxiii–liv. Oxford University Press. https://doi.org/https://doi.org/10.1093/oxfordhb/9780199933624.013.1.

Hodge, James G., and Kim Weidenaar. 2016. "Public Health Emergencies as Threats to National Security." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2844446.

Hoffmann, Stanley. 1995. "The Crisis of Liberal Internationalism." *Foreign Policy* 98: 159-77. https://doi.org/10.2307/1148964.

Holsti, Kal J. 1978. "A New International Politics? Diplomacy in Complex Interdependence." *International Organization* 32 (2): 513–30. https://doi.org/10.1017/S002081830002662X.

— 1986. "The Horsemen of the Apocalypse: At the Gate, Detoured, or Retreating?" *International Studies Quarterly* 30 (4): 355–72. https://doi.org/10.2307/2600639.

— 1992. "Governance without Government: Polyarchy in Nineteenth-Century European International Politics." In *Governance without Government*, edited by James N. Rosenau and Ernst-Otto Czempiel, 30–57. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511521775.004.

Howell, Lee. 2013. "Global Risks 2013. Eighth Edition." 2013. https://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf.

IACG (Interagency Coordination Group on Antimicrobial Resistance). 2019. "No Time to Wait: Securing the Future from Drug-Resistant Infections. Report to the Secretary-General of the United Nations." April. https://www.who.int/publications/i/item/no-time-to-wait-securing-the-future-from-drug-resistant-infections.

INSPI (Instituto Nacional de Investigación en Salud Pública). 2021. "Vigilancia." https://web.archive.org/web/20210301093818/http://www.investigacionsalud.gob.ec/webs/ram/vigilancia-ram

Iván, Gábor, and Vince Grolmusz. 2011. "When the Web Meets the Cell: Using Personalized PageRank for Analyzing Protein Interaction Networks." *Bioinformatics* 27 (3): 405–7. https://doi.org/10.1093/bioinformatics/btq680.

Jasanoff, Sheila. 2004. "Ordering Knowledge, Ordering Society." In *States of Knowledge: The Coproduction of Science and Social Order*, edited by Sheila Jasanoff, 13–45. London: Routledge.

Jervis, Robert. 1982. "Security Regimes." *International Organization* 36 (2): 357–78. http://www.jstor.org/stable/2706526.

Jessop, Bob. 2000. "The Changing Governance of Welfare: Recent Trends in Its Primary Functions, Scale, and Modes of Coordination." In *New Risks, New Welfare: Signposts for Social Policy*, edited by Nick Manning and Ian Shaw, 12–23. Blackwell.

— 2003. "Governance and Metagovernance: On Reflexivity, Requisite Variety, and Requisite Irony." In *Governance, as Social and Political Communication*, edited by Henrik Paul Bang, 142–72. Manchester: Manchester University Press.

Jin, Jiyong, and Joe Thomas Karackattu. 2011. "Infectious Diseases and Securitization: WHO's Dilemma." *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 9 (2): 181–87. https://doi.org/10.1089/bsp.2010.0045.

Kalyagin, Valery A., Panos M. Pardalos, and Themistocles M. Rassias, eds. 2014. *Network Models in Economics and Finance*. Vol. 100. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-09683-4.

Kant, Immanuel. 2006. *Toward Perpetual Peace and Other Writings on Politics, Peace, and History*. Edited by Pauline Kleingeld. Translated by David L. Colclasure. New Haven: Yale University Press.

Kelle, Alexander. 2007. "Securitization of International Public Health: Implications for Global Health Governance and the Biological Weapons Prohibition Regime." *Global Governance: A Review of Multilateralism and International Organizations* 13 (2): 217–35. https://doi.org/10.1163/19426720-01302006.

Kent, Sherman. 1966. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press. https://doi.org/10.1515/9781400879151.

Keohane, Robert O. 1982. “The Demand for International Regimes.” *International Organization* 36 (2): 325–55. http://www.jstor.org/stable/2706525.

— 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press. https://doi.org/10.2307/j.ctt7sq9s.

— 1988. “International Institutions: Two Approaches.” *International Studies Quarterly* 32 (4): 379. https://doi.org/10.2307/2600589.

— 1989. “Neoliberal Institutionalism: A Perspective on World Politics.” In *International Institutions and State Power*. New York: Routledge. https://doi.org/10.4324/9780429032967.

— 2002. *Power and Governance in a Partially Globalized World*. London: Routledge. https://doi.org/10.4324/9780203218174.

Keohane, Robert O., and Joseph S. Nye. 1998. “Power and Interdependence in the Information Age.” *Foreign Affairs* 77 (5). https://doi.org/10.2307/20049052.

— 2012. *Power and Interdependence*. 4th ed. Longman.

Kilpatrick, Dean G. 2004. “Interpersonal Violence and Public Policy: What about the Victims?” *The Journal of Law, Medicine & Ethics* 32 (1): 73–81. https://doi.org/10.1111/j.1748-720X.2004.tb00450.x.

Kirchner, Emil J. 2007. “Regional and Global Security: Changing Threats and Institutional Responses.” In *Global Security Governance*, edited by Emil J. Kirchner and James Sperling. London: Routledge. https://doi.org/10.4324/9780203964705.

Kisby, Ben. 2007. “Analysing Policy Networks: Towards an Ideational Approach.” *Policy Studies* 28 (1): 71–90. https://doi.org/10.1080/01442870601121502.

Kitchin, Rob. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: SAGE Publications Ltd. https://doi.org/10.4135/9781473909472.

Kleinberg, Jon M. 1999. "Authoritative Sources in a Hyperlinked Environment." *Journal of the ACM* 46 (5): 604–32. https://doi.org/10.1145/324133.324140

Kluge, Hans, Jose Maria Martín-Moreno, Nedret Emiroglu, Guenael Rodier, Edward Kelley, Melitta Vujnovic, and Govin Permanand. 2018. "Strengthening Global Health Security by Embedding the International Health Regulations Requirements into National Health Systems." *BMJ Global Health* 3 (Suppl. 1): e000656. https://doi.org/10.1136/bmjgh-2017-000656.

Knoke, David. 1993. "Networks as Political Glue: Explaining Public Policy-Making." In *Sociology and the Public Agenda*, edited by William Julius Wilson, 164–84. Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/10.4135/9781483325484.n9.

Knoke, David, and James H Kuklinski. 1982. *Network Analysis. Quantitative Applications in the Social Sciences*. Beverly Hills, CA: SAGE Publishing.

Knoke, David, and Song Yang. 2008. *Social Network Analysis*. Thousand Oaks, CA: SAGE Publications, Inc. https://doi.org/10.4135/9781412985864.

Kobayashi, Mei, and Koichi Takeda. 2000. "Information Retrieval on the Web." *ACM Computing Surveys* 32 (2): 144–73. https://doi.org/10.1145/358923.358934.

Kooiman, Jan. 2003. *Governing as Governance*. London: SAGE. https://doi.org/10.4135/9781446215012.

Kovacs, Amos. 1997. "Using Intelligence." *Intelligence and National Security* 12 (4): 145–64. https://doi.org/10.1080/02684529708432452.

Krahmann, Elke. 2003. "Conceptualizing Security Governance." *Cooperation and Conflict* 38 (1): 5–26. http://www.jstor.org/stable/45083967.

— 2005. "From State to Non-State Actors: The Emergence of Security Governance." In *New Threats and New Actors in International Security*, edited by Elke Krahmann, 3–19. New York: Palgrave Macmillan US. https://doi.org/10.1057/9781403981660_1.

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36 (2): 185–205. http://www.jstor.org/stable/2706520.

Krasner, Stephen D. 1983. *International Regimes*. Ithaca and London: Cornell University Press.
— 1991. "Global Communications and National Power: Life on the Pareto Frontier." *World Politics* 43 (3): 336–66. https://doi.org/10.2307/2010398
Kuhn, Thomas S. 1996. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press. https://doi.org/10.7208/chicago/9780226458106.001.0001.
Kurzweil, Ray. 2019. "The Deeply Intertwined Promise and Peril of GNR." In *Artificial Intelligence Safety and Security*, edited by Roman V. Yampolskiy, 1st ed. Boca Raton, FL: Chapman and Hall / CRC. https://doi.org/10.1201/9781351251389.
Lachenal, Guillaume. 2013. "Le Stade Dubaï de La Santé Publique." *Revue Tiers Monde* 215 (3): 53. https://doi.org/10.3917/rtm.215.0053.
Lakoff, Andrew. 2008. "The Generic Biothreat, or, How We Became Unprepared." *Cultural Anthropology* 23 (3): 399–428. https://doi.org/10.1111/j.1548-1360.2008.00013.x.
— 2015. "Global Health Security and the Pathogenic Imaginary." In *Dreamscapes of Modernity*, edited by Sheila Jasanoff and Sang-Hyun Kim, 300–320. Chicago, IL: University of Chicago Press. https://doi.org/10.7208/chicago/9780226276663.003.0014.
— 2017. *Unprepared: Global Health in a Time of Emergency*. Oakland, CA: University of California Press. https://doi.org/10.1525/9780520968417.
Lambiotte, Renaud, and Michael T. Schaub. 2022. *Modularity and Dynamics on Complex Networks*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108774116.
Lamont, Christopher. 2015. "Mixed Methods Research in International Relations." In *Research Methods in International Relations*. London: SAGE.
Latour, Bruno. 1987. *Science in Action. How to Follow Scientists and Engineers through Society*. Harvard University Press.
— 1988. *The Pasteurization of France*. Cambridge, MA: Harvard University Press.
— 1993. *We Have Never Been Modern*. Translated by Catherine Porter. Cambridge, MA: Harvard University Press.

Latour, Bruno. 1999. *Pandora's Hope. Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press.

— 2005. *Reassembling the Social – An Introduction to Actor-Network-Theory*. Oxford University Press.

Laumann, Edward O., Peter V. Marsden, and David Prensky. 1983. "The Boundary Specification Problem in Network Analysis." In *Applied Network Analysis: A Methodological Introduction*, edited by Ronald S. Burt and Michael J. Minor, 18–34. Beverly Hills, CA: SAGE.

Law, John. 1984. "On the Methods of Long-Distance Control: Vessels, Navigation and the Portuguese Route to India." *The Sociological Review* 32 (1_suppl): 234–63. https://doi.org/10.1111/j.1467-954X.1984.tb00114.x

— 1992. "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity." *Systems Practice* 5 (4): 379–93. https://doi.org/10.1007/BF01059830.

Law, John, and Vicky Singleton. 2005. "Object Lessons." *Organization* 12 (3): 331–55. https://doi.org/10.1177/1350508405051270.

Star, Susan Leigh. 2010. "This Is Not a Boundary Object: Reflections on the Origin of a Concept." *Science, Technology, & Human Values* 35 (5): 601–17. https://doi.org/10.1177/0162243910377624.

Lessig, Lawrence. 2006. *Code Version 2.0*. New York: Basic Books.

Liao, Danzi. 2013. "Security Governance: An Alternative Paradigm?" *International Journal of Social Science and Humanity*, 17–23. https://doi.org/10.7763/IJSSH.2012.V2.62.

Liotta, Peter H. 2002. "Boomerang Effect: The Convergence of National and Human Security." *Security Dialogue* 33 (4): 473–88. https://doi.org/10.1177/0967010602033004007

Locke, John. 1980. *Second Treatise of Government*. Indianapolis: Hackett Publication Company.

Marsh, David, and Martin Smith. 2000. "Understanding Policy Networks: Towards a Dialectical Approach." *Political Studies* 48 (1): 4–21. https://doi.org/10.1111/1467-9248.00247.

McCarthy, John. 2007. "What Is Artificial Intelligence?". Stanford, CA: Stanford University. http://jmc.stanford.edu/articles/whatisai/whatisai.pdf.

McSweeney, Bill. 1996. "Identity and Security: Buzan and the Copenhagen School." *Review of International Studies* 22 (1): 81–93. https://doi.org/10.1017/S0260210500118467.

Mearsheimer, John J. 1994. "The False Promise of International Institutions." *International Security* 19 (3): 5–49. https://doi.org/10.2307/2539078.

Mertens, Donna M., Patricia Bazeley, Lisa Bowleg, Nigel Fielding, Joseph Maxwell, José F. Molina-Azorin, and Katrin Niglas. 2016. "Expanding Thinking Through a Kaleidoscopic Look Into the Future." *Journal of Mixed Methods Research* 10 (3): 221–27. https://doi.org/10.1177/1558689816649719

Ministerio de Salud Pública del Ecuador. 2014. "Normas del Sistema Integrado de Vigilancia Epidemiológica. Norma técnica." 2014. https://aplicaciones.msp.gob.ec/salud/archivosdigitales/documentosDirecciones/dnn/archivos/EDITOGRAN%20NORMA%20SIVE.pdf.

— 2019a. "Plan Nacional para la prevención y control de la resistencia antimicrobiana 2019-2023." Quito: Viceministerio de Gobernanza y Vigilancia de la Salud. https://www.salud.gob.ec/wp-content/uploads/2019/10/Plan-Nacional-para-la-prevenci%C3%B3n-y-control-de-la-resistencia-antimicrobiana_2019_compressed.pdf.

— 2019b. "Reporte de datos de resistencia a los antimicrobianos en Ecuador 2014-2018." https://www.salud.gob.ec/wp-content/uploads/2019/08/gaceta_ram2018.pdf.

MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones). 2020. "Así funciona CoronApp Colombia, aplicación para detectar y monitorear casos de covid-19." April 14. https://mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/135648:Asi-funciona-CoronApp-Colombia-aplicacion-para-detectar-y-monitorear-casos-de-covid-19.

Mitchell, J. Clyde. 1969. "The Concept and Use of Social Networks." In *Social Networks in Urban Situations: Analyses of Personal Relationships in Central African Towns*, edited by J. Clyde Mitchell. Manchester: Manchester University Press. https://catalog.hathitrust.org/Record/000976657.

Mol, Annemarie, and John Law. 1994. "Regions, Networks and Fluids: Anaemia and Social Topology." *Social Studies of Science* 24 (4): 641–71. http://www.jstor.org/stable/370267.

Mueller, Matthew, and Christopher R. Tainter. 2021. "Escherichia Coli." In *StatPearls [Internet]*. Treasure Island, FL: StatPearls Publishing.

Murch, Randall S., William K. So, Wallace G. Buchholz, Sanjay Raman, and Jean Peccoud. 2018. "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy." *Frontiers in Bioengineering and Biotechnology* 6 (April). https://doi.org/10.3389/fbioe.2018.00039.

National Academies of Sciences, Engineering, and Medicine. 2015. "Safeguarding the Bioeconomy: Applications and Implications of Emerging Science. Meeting Recap. July 27-28, 2015." Washington, DC: National Academies Press. https://www.ehidc.org/resources/safeguarding-bioeconomy-applications-and-implications-emerging-science-meeting-recap-july.

— 2020. *Safeguarding the Bioeconomy*. 9th ed. Washington, DC: The National Academies Press. https://doi.org/10.17226/25525.

National Health Commission. 2021. "China Antimicrobial Resistance Surveillance System (CARSS in Chinese)." https://web.archive.org/web/20240915194032/https://www.carss.cn/

Nye, Joseph S., and Robert O. Keohane. 1971. "Transnational Relations and World Politics: An Introduction." *International Organization* 25 (3): 329–49. https://doi.org/10.1017/S0020818300026187.

O Presidente da República. 2020. "LEI No 13.979, DE 6 DE FEVEREIRO DE 2020." Diário Oficial Da Uniáo. República Federativa Do Brasil - Imprensa Nacional. https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=07/02/2020&jornal=515&pagina=1.

O'Brien, Thomas F., and John M. Stelling. 1995. "WHONET: An Information System for Monitoring Antimicrobial Resistance." *Emerging Infectious Diseases* 1 (2): 66–66. https://doi.org/10.3201/eid0102.950209.

OECD. 2021. *Health at a Glance 2021: OECD Indicators*. Paris: OECD Publishing. https://doi.org/10.1787/ae3016b9-en.

Oliveira, Gilberto Carvalho. 2018. "The Causal Power of Securitisation: An Inquiry into the Explanatory Status of Securitisation Theory Illustrated by the Case of Somali Piracy." *Review of International Studies* 44 (3): 504–25. https://doi.org/10.1017/S0260210517000559.

Omohundro, Stephen M. 2018. "The Basic AI Drives." In *Artificial Intelligence Safety and Security*, edited by Roman V. Yampolskiy, 47–56. Boca Raton, FL: Chapman and Hall/CRC. https://doi.org/10.1201/9781351251389.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY: Crown Publishing Group.

O'Neill, Jim. 2014. "Antimicrobial Resistance: Tackling a Crisis for the Health and Wealth of Nations." *Review on Antimicrobial Resistance*. December 2014. https://wellcomecollection.org/works/rdpck35v.

Orsini, Amandine, Sélim Louafi, and Jean-Frédéric Morin. 2017. "Boundary Concepts for Boundary Work Between Science and Technology Studies and International Relations: Special Issue Introduction." *Review of Policy Research* 34 (6): 734–43. https://doi.org/10.1111/ropr.12273.

Ortega-Paredes, David, Sofía de Janon, Fernando Villavicencio, Katherine Jaramillo Ruales, Kenny De La Torre, José E. Villacís, Jaap A. Wagenaar, Jorge Matheu, Camila Bravo-Vallejo, Esteban Fernández-Moreira, and Christian Vinueza-Burgos. 2020. "Broiler Farms and Carcasses Are an Important Reservoir of Multi-Drug Resistant Escherichia Coli in Ecuador." *Frontiers in Veterinary Science* 7 (November). https://doi.org/10.3389/fvets.2020.547843.

O'Toole, Marie T. 2013. *Mosby's Medical Dictionary*. Edited by Marie T. O'Toole. Elsevier.

Page, Edward C. 2008. "The Origins of Policy." In *The Oxford Handbook of Public Policy*, edited by Robert E. Goodin, Michael Moran, and Martin Rein, 207–27. Oxford University Press.

Pan American Health Organization. 2021. "Considerations for Strengthening the First Level of Care in the Management of the COVID-19 Pandemic." Washington, DC: PAHO. https://iris.paho.org/handle/10665.2/53190.

Panda Security. 2017. "PandaLabs Quarterly Report: Q2 2017." Madrid. https://www.pandasecurity.com/mediacenter/src/uploads/2017/08/Pandalabs-2017-Q2-EN.pdf.

Pando, Diego, and Eduardo Poggi. 2020. "Datos masivos para la toma de decisiones públicas: aportes para un debate imprescindible." In *Desafíos de la administración pública en el contexto de la revolución 4.0*, edited by Santiago Bellomo and Oscar Oszlak, 243–64. Ciudad Autónoma de Buenos Aires: Konrad Adenauer Stiftung.

Peccoud, Jean, Jenna E. Gallegos, Randall Murch, Wallace G. Buchholz, and Sanjay Raman. 2018. "Cyberbiosecurity: From Naive Trust to Risk Awareness." *Trends in Biotechnology* 36 (1): 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012.

Perra, Nicola, and Santo Fortunato. 2008. "Spectral Centrality Measures in Complex Networks." *Physical Review* E 78 (3): 036107. https://doi.org/10.1103/PhysRevE.78.036107.

Pestre, Dominique. 2012. "Debates in Transnational and Science Studies: A Defence and Illustration of the Virtues of Intellectual Tolerance." *The British Journal for the History of Science* 45 (3): 425–42. https://doi.org/10.1017/S0007087412000386.

Peters, B. Guy. 2007. "Globalization, Governance, and the State: Some Propositions about Governing." *Iberoamericana – Nordic Journal of Latin American and Caribbean Studies* 37 (1): 19. https://doi.org/10.16993/ibero.194.

Pfizer. 2020a. "Biopharma Leaders Unite To Stand With Science." September 8. https://www.pfizer.com/news/press-release/press-release-detail/biopharma-leaders-unite-stand-science.

— 2020b. "Pfizer Outlines Five-Point Plan to Battle COVID-19." March 13. https://www.pfizer.com/news/press-release/press-release-detail/pfizer-outlines-five-point-plan-battle-covid-19.

Piddock, Laura J. V., Jean-Pierre Paccaud, Seamus O'Brien, Michelle Childs, Rohit Malpani, and Manica Balasegaram. 2022. "A Nonprofit Drug Development Model Is Part of the Antimicrobial Resistance (AMR) Solution." *Clinical Infectious Diseases* 74 (10): 1866–71. https://doi.org/10.1093/cid/ciab887.

Pierre, Jon. 2000. "Introduction: Understanding Governance." In *Debating Governance: Authority, Steering, and Democracy*, edited by Jon Pierre, 1–10. Oxford University Press. https://doi.org/10.1093/oso/9780198295143.003.0001.

Pierre, Jon, and B. Guy Peters. 2005. *Governing Complex Societies*. London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230512641.

Pironti, John P. 2007. "Developing Metrics for Effective Information Security Governance." *Information Systems Control Journal* 2. http://iparchitects.com/wp-content/uploads/2016/07/Developing-Metrics-and-Measures-for-Information-Security-Governance-ISACA-Member-Journal-March-2007.pdf.

Plato. 1941. *The Republic*. Translated by Benjamin Jowett. New York, NY: The Modern Library.

Presidencia de la Nación. República Argentina. 2020. "Emergencia sanitaria 260/2020 DECNU-2020-260-APN-PTE - Coronavirus (COVID-19). Disposiciones." Buenos Aires: Presidencia de la Nación. República Argentina. March 12. https://www.boletinoficial.gob.ar/detalleAviso/primera/5217883/20200312?busqueda=3&suplemento=1.

Presidencia de la República del Ecuador. 2020. "Decreto Ejecutivo 1017." Quito. March 16. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Decreto_presidencial_No_1017_17-Marzo-2020.pdf.

Presidencia del Consejo de Ministros. 2020. "Decreto Supremo N.° 044-2020-PCM." March 15. https://www.gob.pe/es/l/460472.

Puchala, Donald J., and Raymond F. Hopkins. 1982. "International Regimes: Lessons from Inductive Analysis." *International Organization* 36 (2): 245–75. https://doi.org/10.1017/S0020818300018944.

Quet, Mathieu. 2021. *Illicit Medicines in the Global South*. London: Routledge. https://doi.org/10.4324/9781003194767.

Ravitch, Sharon, and Matthew Riggan. 2012. *Reason & Rigor: How Conceptual Frameworks Guide Research*. SAGE. https://doi.org/10.12698/cpre.ReasonandRigor.

ReLAVRA. 2014. "2. Resistance Percentages for Selected Pathogens." 2014. https://www3.paho.org/data/index.php/en/mnu-topics/antimicrobial-resistance/571-amr-vig-en.html.

Rosenau, James N. 1992. "Governance, Order, and Change in World Politics." In *Governance without Government: Order and Change in World Politics*, edited by James N. Rosenau and Ernst-Otto Czempiel, 1–29. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511521775.003.

— 2000. "Change, Complexity, and Governance in Globalizing Space." In *Debating Governance: Authority, Steering, and Democracy*, edited by Jon Pierre, 167–200. Oxford University Press. https://doi.org/10.1093/oso/9780198295143.003.0008.

Ruggie, John Gerard. 1975. "International Responses to Technology: Concepts and Trends." *International Organization* 29 (3): 557–83. https://doi.org/10.1017/S0020818300031696.

Saint-Pierre, Héctor Luis. 2017. "Amenaza: Concepto, clasificación y proceso de securitización." In *Amenazas globales, consecuencias locales. Retos para la inteligencia estratégica actual*, edited by Centro de Estudios Estratégicos, 7–32. Sangolquí: Centro de Estudios Estratégicos - Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/handle/21000/13765.

Salvatierra-González, Roxane, and Manuel Guzmán-Blanco. 1999. "Conferencia Panamericana de Resistencia Antimicrobiana en las Américas." *Revista Panamericana de Infectología* 3 (1).

Samimian-Darash, Limor, Hadas Henner-Shapira, and Tal Daviko. 2016. "Biosecurity as a Boundary Object: Science, Society, and the State." *Security Dialogue* 47 (4): 329–47. https://doi.org/10.1177/0967010616642918.

Sanche, Steven, Yen Ting Lin, Chonggang Xu, Ethan Romero-Severson, Nick Hengartner, and Ruian Ke. 2020. "High Contagiousness and Rapid Spread of Severe Acute Respiratory Syndrome Coronavirus 2." *Emerging Infectious Diseases* 26 (7): 1470–77. https://doi.org/10.3201/eid2607.200282.

Sanclemente, Gaudys L. 2018. "The Applicable Use of Mixed Methods in Big Data Analysis (Essay)." FLACSO Ecuador.

— 2022. "Reliability: Understanding Cognitive Human Bias in Artificial Intelligence for National Security and Intelligence Analysis." *Security Journal* 35 (4): 1328–48. https://doi.org/10.1057/s41284-021-00321-2.

Sandström, Annica, and Lars Carlsson. 2008. "The Performance of Policy Networks: The Relation between Network Structure and Network Performance." *Policy Studies Journal* 36 (4): 497–524. https://doi.org/10.1111/j.1541-0072.2008.00281.x.

Satter, Raphael, Jack Stubbs, and Christopher Bing. 2020. "Exclusive: Elite Hackers Target WHO as Coronavirus Cyberattacks Spike." Reuters. March 23. https://www.reuters.com/article/technology/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21B07J/.

Scanvic, Agnès, Ljiljiana Denic, Stéphanie Gaillon, Pascal Giry, Antoine Andremont, Jean-Christophe Lucet. 2001. "Duration of Colonization by Methicillin-Resistant Staphylococcus Aureus after Hospital Discharge and Risk Factors for Prolonged Carriage." *Clinical Infectious Diseases* 32 (10): 1393–98. https://doi.org/10.1086/320151.

Scott, Hayley, Aleena Zahra, Rafael Fernandes, Bettina C. Fries, Henry C. Thode, and Adam J. Singer. 2022. "Bacterial Infections and Death among Patients with Covid-19 versus Non Covid-19 Patients with Pneumonia." *The American Journal of Emergency Medicine* 51 (January): 1–5. https://doi.org/10.1016/j.ajem.2021.09.040.

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs.

Smith, Adam. 2000. *The Wealth of Nations*. Edited by Edwin Cannan. New York, NY: Modern Library.

Sperling, James, and Mark Webber. 2014. "Security Governance in Europe: A Return to System." *European Security* 23 (2): 126–44. https://doi.org/10.1080/09662839.2013.856305.

Stake, Robert E. 1995. *The Art of Case Study Research*. Thousand Oaks, CA: SAGE Publishing.

Star, Susan Leigh, and James R. Griesemer. 1989. "Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39." *Social Studies of Science* 19 (3): 387–420. https://doi.org/10.1177/030631289019003001.

Star, Susan Leigh, and Karen Ruhleder. 1996. "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces." *Information Systems Research* 7 (1): 111–34. https://doi.org/10.1287/isre.7.1.111.

Steadman, Ian. 2013. "Big Data and the Death of the Theorist." Wired. January 25. https://www.wired.com/story/big-data-end-of-theory/.

Stein, Arthur A. 1982. "Coordination and Collaboration: Regimes in an Anarchic World." *International Organization* 36 (2): 299–324. https://doi.org/10.1017/S0020818300018968.

— 2008. "Neoliberal Institutionalism." In *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal, 201–21. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199219322.003.0011.

Stelling, J., W. K. Yih, M. Galas, M. Kulldorff, M. Pichel, R. Terragno, E. Tuduri, S. Espetxe, N. Binsztein, T. F. O'Brien, R. Platt, and Collaborative Group WHONET-Argentina. 2010. "Automated Use of WHONET and SaTScan to Detect Outbreaks of Shigella Spp. Using Antimicrobial Resistance Phenotypes." *Epidemiology and Infection* 138 (6): 873–83. https://doi.org/10.1017/S0950268809990884.

Strange, Susan. 1983. "Cave! Hic Dragones: A Critique of Regime Analysis." In *International Regimes*, edited by Stephen D. Krasner, 337–54. New York, NY: Cornell University Press.

Šulović, Vladimir. 2010. "Meaning of Security and Theory of Securitization." Belgrade: Belgrade Centre for Security Policy. https://bezbednost.org/en/publication/meaning-of-security-and-the-theory-of-securitization/.

Taylor, Tracey A., and Chandrashekhar G. Unakal. 2021. "Staphylococcus Aureus." In *StatPearls [Internet]*. Treasure Island, FL: StatPearls Publishing.

The White House. 2012. "National Bioeconomy Blueprint." April. https://obamawhitehouse.archives.gov/administration/eop/ostp/library/bioeconomy.

— 2014. "National Strategy for Combating Antibiotic-Resistant Bacteria." September.

The White House. 2012. "National Action Plan for Combating Antibiotic-Resistant Bacteria." April. https://obamawhitehouse.archives.gov/the-press-office/2015/03/27/fact-sheet-obama-administration-releases-national-action-plan-combat-ant.

— 2020. "G7 Leaders' Statement." March 16. https://trumpwhitehouse.archives.gov/briefings-statements/g7-leaders-statement.

Thompson, John R., R. Hopf-Weichel, and R.E. Geiselman. 1984. "The Cognitive Bases of Intelligence Analysis." Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences. https://apps.dtic.mil/sti/tr/pdf/ADA146132.pdf.

Tomczyk, Sara, Angelina Taylor, Allison Brown, Marlieke E. A. de Kraker, Aiman El-Saed, Majid Alshamrani, Rene S. Hendriksen, Megan Jacob, Sonja Löfmark, Olga Perovic, Nandini Shetty, Dawn Sievert, Rachel Smith, John Stelling, Siddhartha Thakur, Ann Christin Vietor, and Tim Eckmanns. 2021. "Impact of the COVID-19 Pandemic on the Surveillance, Prevention and Control of Antimicrobial Resistance: A Global Survey." *Journal of Antimicrobial Chemotherapy* 76 (11): 3045–58. https://doi.org/10.1093/jac/dkab300.

United Nations. 2019a. "The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation." New York, NY. http://digitallibrary.un.org/record/3865925/files/DigitalCooperation-report.pdf.

— 2019b. "World Population Prospects 2019: Highlights (ST/ESA/SER.A/423)." https://population.un.org/wpp/assets/Files/WPP2019_Highlights.pdf.

United Nations Office for Disarmament Affairs. 2021. "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." July 14. https://digitallibrary.un.org/record/3934214/files/A_76_135-EN.pdf.

U.S. Congress. House of Representatives. 2018. "Game Changers: Artificial Intelligence Part I." 115th Cong., 2nd Sess. February 14. https://www.govinfo.gov/app/details/CHRG-115hhrg30296/CHRG-115hhrg30296.

U.S. Congress. Senate. 2016. "The Dawn of Artificial Intelligence." 114th Cong., 2nd Sess. November 30. https://www.govinfo.gov/app/details/CHRG-114shrg24175/CHRG-114shrg24175.

U.S. Department of Health and Human Services. 2020a. "September 9-10, 2020 Virtual Public Meeting – Antimicrobial Resistance and COVID-19." September 10. https://www.hhs.gov/ash/advisory-committees/paccarb/meetings/upcoming-meetings/september-9-2020-virtual-public-meeting.html.

— 2020b. "February 26-27, 2020 - HHS Listening Sessions." February 27. https://www.hhs.gov/ash/advisory-committees/paccarb/meetings/upcoming-meetings/february-26-2020-hhs-listening-sessions/index.html.

— 2020c. "Secretary Azar Declares Public Health Emergency for United States for 2019 Novel Coronavirus." January 31. https://public3.pagefreezer.com/content/HHS.gov/16-09-2020T14:35/https://www.hhs.gov/about/news/2020/01/31/secretary-azar-declares-public-health-emergency-us-2019-novel-coronavirus.html.

U.S. Department of Homeland Security. 2020. "Final Report: Emerging Technologies Subcommittee Quantum Information Science." November 2020. https://www.dhs.gov/sites/default/files/publications/final_emerging_technologies_quantom_report_1.pdf.

— 2022. *DHS National Biosurveillance Integration Center State, Local, Tribal, and Territorial Engagement Strategy, FY 2022-2025*. https://web.archive.org/web/20240929090618/https://www.dhs.gov/sites/default/files/2023-08/23_0801_cwmd_nbic-sltt-engagement-strategy-final.pdf

U.S. Director of National Intelligence. 2006. "Inteligence Community Directive Number 301." July 11. https://irp.fas.org/dni/icd/icd-301.pdf.

— 2019. "National Intelligence Strategy of the United States of America." Washington, DC: Office of the Director of National Intelligence. https://www.intelligence.gov/templates/intelgov-template/custom-sections/the-nis-at-a-glance/nis-2023/pdf/nis-2019.pdf.

Vinck, Dominique. 2010. *The Sociology of Scientific Work*. Cheltenham: Edward Elgar Publishing. https://doi.org/10.4337/9781849807197.

Viotti, Paul R., and Mark V. Kauppi. 2012. *International Relations Theory*. Longman.

Viotti, Paul R., and Mark V. Kauppi. 2020. *International Relations Theory*. 6th ed. Maryland: Rowman & Littlefield.

Waltz, Kenneth. 1979. *Theory of International Politics*. Reading, MA: Addison–Wesley Publishing Company.

Wang, Jiancong, M. Zhou, G. Huang, Z. Guo, J. Sauser, Aliki Metsini, Didier Pittet, and Walter Zingg. 2020. "Antimicrobial Resistance in Southern China: Results of Prospective Surveillance in Dongguan City, 2017." *Journal of Hospital Infection* 105 (2): 188–96.

Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511815478.

Wastell, Colin A. 2010. "Cognitive Predispositions and Intelligence Analyst Reasoning." *International Journal of Intelligence and CounterIntelligence* 23 (3): 449–60. https://doi.org/10.1080/08850601003772802.

Webb, Amy. 2019. *The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity*. New York, NY: PublicAffairs.

Webber, Mark, Stuart Croft, Jolyon Howorth, Terry Terriff, and Elke Krahmann. 2004. "The Governance of European Security." *Review of International Studies* 30 (1): 3–26. https://doi.org/10.1017/S0260210504005807.

Weizenbaum, Joseph. 1976. *Computer Power and Human Reason: From Judgement to Calculation*. New York, NY: W. H. Freeman & Company.

Wi, Teodora, Monica M. Lahra, Francis Ndowa, Manju Bala, Jo-Anne R. Dillon, Pilar Ramon-Pardo, Sergey R. Eremin, Gail Bolan, and Magnus Unemo. 2017. "Antimicrobial Resistance in Neisseria Gonorrhoeae: Global Surveillance and a Call for International Collaborative Action." *PLOS Medicine* 14 (7): e1002344. https://doi.org/10.1371/journal.pmed.1002344.

Wiener, Norbert. 1989. *The Human Use of Human Beings*. London: Free Association Books.

Winner, Langdon. 1986. *The Whale and the Reactor: A Search for Limits in an Age of High Technology, Second Edition*. Chicago, IL: The University of Chicago Press.

Wolfers, Arnold. 1962. *Discord and Collaboration: Essays on International Politics*. Baltimore, MA: The Johns Hopkins Press.

Worby, Colin J., Dakshika Jeyaratnam, Julie V. Robotham, Theodore Kypraios, Philip D. O'Neill, Daniela De Angelis, Gary French, and Ben S. Cooper. 2013. "Estimating the Effectiveness of Isolation and Decolonization Measures in Reducing Transmission of Methicillin-Resistant Staphylococcus Aureus in Hospital General Wards." *American Journal of Epidemiology* 177 (11): 1306–13. https://doi.org/10.1093/aje/kws380.

World Health Organization. 2001. "WHO Global Strategy for Containment of Antimicrobial Resistance." https://iris.who.int/handle/10665/66860.

— 2004. "Public Health Response to Biological and Chemical Weapons. WHO Guidance." https://www.who.int/publications/i/item/public-health-response-to-biological-and-chemical-weapons-who-guidance-(2004).

— 2014. "Antimicrobial Resistance: Global Report on Surveillance." World Health Organization. https://iris.who.int/handle/10665/112642.

— 2015a. "World Health Organization: Global Antimicrobial Resistance Surveillance System (GLASS) Terms of Use."

— 2015b. "Global Action Plan on Antimicrobial Resistance." https://www.who.int/publications/i/item/9789241509763.

— 2015c. "Global Antimicrobial Resistance Surveillance System: Manual for Early Implementation." https://iris.who.int/handle/10665/188783.

— 2015d. "Sixty-Eighth World Health Assembly." May 26. https://apps.who.int/gb/ebwha/pdf_files/WHA68-REC1/A68_R1_REC1-en.pdf#page=1.

— 2016a. *International Health Regulations (2005)*. 3rd ed. https://iris.who.int/handle/10665/246107

— 2016b. "National Antimicrobial Resistance Surveillance Systems and Participation in the Global Antimicrobial Resistance Surveillance System (GLASS): A Guide to Planning, Implementation, and Monitoring and Evaluation. WHO/DGO/AMR/2016.4." https://iris.who.int/handle/10665/251554

— 2016c. "United Nations Meeting on Antimicrobial Resistance." *Bulletin of the World Health Organization* 94 (9): 638–39. https://pmc.ncbi.nlm.nih.gov/articles/PMC5034641/pdf/BLT.16.020916.pdf

World Health Organization. 2016d. "GLASS Country Profiles, 2016." https://web.archive.org/web/20180202220046/https://www.who.int/glass/country-participation/en/

— 2017a. *Critically Important Antimicrobials for Human Medicine: Ranking of Antimicrobial Agents for Risk Management of Antimicrobial Resistance Due to Non-Human Use*. 5th Rev. https://iris.who.int/handle/10665/255027.

— 2017b. "Global Antimicrobial Resistance Surveillance System (GLASS) Report: Early Implementation 2016-2017." https://iris.who.int/handle/10665/259744.

— 2017c. "Global Priority List of Antibiotic-Resistant Bacteria to Guide Research, Discovery, and Development of New Antibiotics." https://remed.org/wp-content/uploads/2017/03/lobal-priority-list-of-antibiotic-resistant-bacteria-2017.pdf.

—2017d. "Prioritization of Pathogens to Guide Discovery, Research and Development of New Antibiotics for Drug-Resistant Bacterial Infections, Including Tuberculosis. WHO/EMP/IAU/2017.12." https://iris.who.int/handle/10665/311820.

— 2017e. "2nd High Level Technical Meeting on Surveillance of Antimicrobial Resistance for Local and Global Action." https://www.who.int/publications/m/item/surveillance-of-antimicrobial-resistance-for-local-and-global-action---2nd-high-level-technical-meeting.

— 2017f. "World Health Statistics 2017: Monitoring Health for the SDGs, Sustainable Development Goals." https://iris.who.int/handle/10665/255336.

— 2018a. "Global Antimicrobial Resistance Surveillance System (GLASS) Report: Early Implementation 2017-2018." https://iris.who.int/handle/10665/279656.

— 2018b. "The World Health Organization: Working for Better Health for Everyone, Everywhere." https://iris.who.int/handle/10665/272468.

— 2018c. "World Health Statistics 2018: Monitoring Health for the SDGs, Sustainable Development Goals." https://iris.who.int/handle/10665/272596.

World Health Organization. 2018d. "WHO Results Report: Programme Budget 2016-2017." https://iris.who.int/handle/10665/276529.
— 2019a. "World Health Assembly Update, 23 May 2019." https://www.who.int/news/item/23-05-2019-world-health-assembly-update-23-may-2019.
— 2019b. "Ten Threats to Global Health in 2019." https://www.who.int/news-room/spotlight/ten-threats-to-global-health-in-2019.
— 2019c. "WHO and Wellcome Trust Join Forces to Combat Epidemics and Drug-Resistant Infections." May 15. https://www.who.int/news/item/15-05-2019-who-and-wellcome-trust-join-forces-to-combat-epidemics-and-drug-resistant-infections.
— 2020a. "Antibiotic Resistance: Key Facts." https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance
— 2020b. "Antimicrobial Resistance Key Facts."
— 2020c. "Beware of Criminals Pretending to Be WHO." https://www.who.int/about/cybersecurity.
— 2020d. "Commitment and Call to Action: Global Collaboration to Accelerate New COVID-19 Health Technologies." May 24. https://www.who.int/news/item/24-04-2020-commitment-and-call-to-action-global-collaboration-to-accelerate-new-covid-19-health-technologies.
— 2020e. "Coronavirus Disease 2019 (COVID-19): Situation Report, 85." https://iris.who.int/handle/10665/331783.
— 2020f. "Weekly Epidemiological Update - 29 December 2020." https://www.who.int/publications/m/item/weekly-epidemiological-update---29-december-2020.
— 2020g. "Global Antimicrobial Resistance Surveillance System (GLASS) Report: Early Implementation 2020." https://iris.who.int/handle/10665/332081.
— 2020h. "Novel Coronavirus (2019-NCoV): Situation Report, 1." https://iris.who.int/handle/10665/330760.
— 2020i. "Novel Coronavirus (2019-NCoV): Situation Report, 11." https://iris.who.int/handle/10665/330776.
— 2020j. "Coronavirus Disease 2019 (COVID-19): Situation Report, 38." https://iris.who.int/handle/10665/331226.

World Health Organization. 2020k. "Coronavirus Disease 2019 (COVID-19): Situation Report, 41." https://iris.who.int/handle/10665/331352.

— 2020l. "Coronavirus Disease 2019 (COVID-19): Situation Report, 44." https://iris.who.int/handle/10665/331355.

— 2020m. "Coronavirus Disease 2019 (COVID-19): Situation Report, 47." https://iris.who.int/handle/10665/331444.

— 2020n. "Coronavirus Disease 2019 (COVID-19) Situation Report – 49." March 9. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200309-sitrep-49-covid-19.pdf.

— 2020o. "Coronavirus Disease 2019 (COVID-19): Situation Report, 51." https://iris.who.int/handle/10665/331475.

— 2020p. "Coronavirus Disease 2019 (COVID-19): Situation Report, 53." https://iris.who.int/handle/10665/331477.

— 2020q. "Coronavirus Disease 2019 (COVID-19): Situation Report, 54." https://iris.who.int/handle/10665/331478.

— 2020r. "Coronavirus Disease 2019 (COVID-19): Situation Report, 56." https://iris.who.int/handle/10665/331480.

— 2020s. "Coronavirus Disease (COVID-19): Situation Report, 193." https://iris.who.int/handle/10665/333727.

— 2020t. "Pneumonia of Unknown Cause – China." January 5. https://www.who.int/emergencies/disease-outbreak-news/item/2020-DON229.

— 2020u. "Public Statement for Collaboration on COVID-19 Vaccine Development." April 13. https://www.who.int/news/item/13-04-2020-public-statement-for-collaboration-on-covid-19-vaccine-development.

— 2020v. "Naming the Coronavirus Disease (COVID-19) and the Virus That Causes It." https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it.

— 2020w. "WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 - 11 March 2020." https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

World Health Organization. 2020x. “Coronavirus Press Conference 11 February, 2020.” https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-full-press-conference-11feb2020-final.pdf.

— 2020y. “3rd High Level Technical Consultation and Meeting on Surveillance of Antimicrobial Resistance and Use for Concerted Actions.” October 22. https://www.who.int/news-room/articles-detail/3rd-member-states-technical-consultation-on-surveillance-of-amr.

— 2021a. “Ageing and Health.” October 1. https://www.who.int/news-room/fact-sheets/detail/ageing-and-health.

— 2021b. “Call to Action on Antimicrobial Resistance 2021.” July 30. https://www.who.int/news/item/30-07-2021-call-to-action-on-antimicrobial-resistance-2021.

— 2021c. “Weekly Epidemiological Update - 23 February 2021.” https://www.who.int/publications/m/item/weekly-epidemiological-update---23-february-2021.

— 2021d. “Global Antimicrobial Resistance and Use Surveillance System (GLASS) Report: 2021.” https://iris.who.int/handle/10665/341666.

— 2021e. “Weekly Operational Update on COVID-19 - 25 October 2021.” https://www.who.int/publications/m/item/weekly-operational-update-on-covid-19---25-october-2021.

— 2021f. “Weekly Operational Update on COVID-19 - 26 July 2021.” https://www.who.int/publications/m/item/weekly-operational-update-on-covid-19---26-july-2021.

— 2021g. “WHO COVID-19 Dashboard.” https://data.who.int/dashboards/covid19/cases?n=c.

—. 2021h. “WHO Director-General’s Remarks at the Member State Briefing on the Report of the International Team Studying the Origins of SARS-CoV-2.” https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-the-member-state-briefing-on-the-report-of-the-international-team-studying-the-origins-of-sars-cov-2.

— 2021i. “Antimicrobial Resistance. Key Facts” November 21. https://www.who.int/docs/default-source/antimicrobial-resistance/amr-fact-sheet.pdf

World Health Organization. 2022. "Who We Are." https://www.who.int/about/who-we-are.

Young, Oran R. 1969. "Interdependencies in World Politics." *International Journal: Canada's Journal of Global Policy Analysis* 24 (4): 726–50. https://doi.org/10.1177/002070206902400407.

— 1982. "Regime Dynamics: The Rise and Fall of International Regimes." *International Organization* 36 (2): 277–97. https://doi.org/10.1017/S0020818300018956.

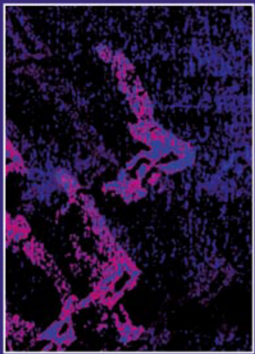
— 1992. "The Effectiveness of International Institutions: Hard Cases and Critical Variables." In *Governance without Government*, edited by James N. Rosenau and Ernst-Otto Czempiel, 160–94. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511521775.008.

Zacher, Mark W. 1992. "The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance." In *Governance without Government*, edited by James N. Rosenau and Ernst-Otto Czempiel, 58–101. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511521775.005.

Zambrano, Ela. 2018. "The Sustainable Bioeconomy, a Path Towards Post-Extractivism." Inter Press Service, July 20. https://www.ipsnews.net/2018/07/sustainable-bioeconomy-path-towards-post-extractivism.

Zurita, Jeannete, Carlos Mejía, and Manuel Guzmán-Blanco. 2010. "Diagnosis and Susceptibility Testing of Methicillin-Resistant Staphylococcus Aureus in Latin America." *Brazilian Journal of Infectious Diseases* 14 (December): 97–106. https://doi.org/10.1590/S1413-86702010000800005.

Printed in June 2025
by V&M Gráficas
Quito, Ecuador



Security governance surrounding infectious diseases necessitates collaboration and information sharing among diverse actors, including nation-states and institutions. The Global Antimicrobial Resistance Surveillance System (GLASS), a form of open-source intelligence, facilitates collaboration among participating countries and enables effective monitoring of infectious diseases. However, this interconnectedness also creates vulnerabilities, opening channels for nontraditional threats ranging from cybercrimes to potential biological attacks.

Gaudys L. Sanclemente analyses how the emergence of unconventional threats, such as the COVID-19 pandemic and antimicrobial resistance, activates security governance, emphasizing the critical role of collaborative dynamics enabled by the open data exchange facilitated by GLASS.

By contributing to the fields of international relations, security, cybersecurity, science, technology, health, and network science, this book provides valuable insights into the complexities of safeguarding global health in an era increasingly defined by technological advancements and emerging threats.

ISBN: 978-9978-67-704-9
9 789978 677049

Editorial FLACSO Ecuador