October 2025
issue brief
Foundation Office Washington, D.C.

KONRAD ADENAUER STIFTUNG

Cybersecuring the Modern Bioeconomy

Policy Imperatives for the AI-Genomics Convergence

Eleonore Pauwels

This policy analysis is based on a high-level panel that took place on April 16, 2025. Gratitude is extended to the following experts and panelists for their invaluable, sharp and visionary insights that helped turn this paper into a forward-looking, actionable, policy analysis.

Sultan Meghji *is Co-Founder and CEO of the secured AI firm Frontier Foundry. He previously served as Chief Innovation Officer at the FDIC, was a scholar at the Carnegie Endowment for International Peace, and a professor at Duke University. He is a globally recognized expert in AI, biotechnology, cybersecurity, quantum computing, and Web3.*

Dr. Sofonias Tessema *is a public health genomic epidemiologist with extensive expertise in molecular diagnostics, genome sequencing, and bioinformatics. At Africa CDC, Dr Tessema leads the Africa Pathogen Genomics Initiative (Africa PGI) that is catalyzing genomics, AI and bioinformatics capacity building in Africa.*

Dr. Sterling Sawaya *is founder and CEO of GeneInfoSec, a startup focused on protecting genetic information with patented molecular cryptographic methods. With expertise in bioinformatics, statistics, and biochemistry, Dr. Sawaya was a 2019-2020 fellow at John Hopkins Center for Health Security and also serves on the consulting advisory board at Merrick and Company.*

Executive Summary

No easy historical reference captures the impact of artificial intelligence (AI) on the living world, from biology itself, to ecosystems, to mammals and microbes, to humans and bio-industries. The convergence of AI and biotechnology holds the secrets to design, rewrite and optimize life on our planet. Boosted by this convergence, the bioeconomy relies on a technological revolution powered to reshape our world at molecular scale. The bio-economy also constitutes a knowledge revolution which produces large-scale datasets, unveils crucial insights and intelligence into how we can optimize biology for better human, industrial, and environmental resilience.

As AI and biotechnology converge and bring new designs to life in digital spaces, these technologies are increasingly vulnerable to cyberthreats. The modern bio-economy depends on vast, interconnected networks of data and software, which are susceptible to cyberattacks capable of undermining not just specific systems and sectors, but entire societal infrastructures in health, agriculture and across industries. As AI systems automate and integrate deeper into biotechnology, they open new avenues for threat actors to manipulate or corrupt sensitive datasets, as well as compromise critical operations, from clinical trials, drug-discovery and development, to biomanufacturing. Protecting the integrity of these critical infrastructures from evolving, enhanced cyberoffense will require governments and private actors to recalibrate their approach to cybersecurity—developing

solutions that account for the specific cyber risks posed by the convergence of AI and biotechnology (increasingly abbreviated in policy circles as "AI-biotech" or "AI x Bio").

As AI and biotechnology integrate in cyberspace, the stakes for national security and global stability are escalating rapidly. **In April 2025, with the support of the Konrad-Adenauer-Stiftung, Foundation Office USA (KAS USA), Eleonore Pauwels published "AI x Biotech: Its Cybersecurity Implications," a report that analyses these challenges from both, a transatlantic and a global perspective.** The bio-economy has become a strategic domain where economic power, security, and technological innovation intersect. The question, then, is not only whether these technologies will reshape global politics, but also how nations will navigate the complex dual-use risks they present.

While many governments acknowledge that the bioeconomy now functions as *de facto* critical infrastructure, policy and regulatory frameworks have not kept pace—especially in cybersecurity. In an April 16 Panel launching the KAS USA report, three experts provided salient points for moving forward:

- Sultan Meghji emphasized the extent to which AI systems and next-generation genomic tools are already globally distributed, commoditized, and vulnerable. He called attention to how quantum computing and more advanced AI will soon exacerbate these threats if left unaddressed.
- Dr. Sterling Sawaya highlighted new molecular cryptography, data classification, and security-by-design practices that could help mitigate dual-use risks, especially by preventing adversaries from easily reconstructing dangerous pathogens or harvesting personal genomic data for malicious ends.
- Dr. Sofonias Tessema urged that Africa's rapid adoption of next-generation genomic sequencing, driven by public health needs and leapfrogging opportunities, must be matched by equally robust national and regional cybersecurity architectures. He warned that without commensurate investment in security, the continent—and indeed, all emerging bio-economies—could become inadvertent testing grounds for exploitation and proliferation.

The present policy paper, drawing on the arguments of these three experts and on the broader analysis introduced by Eleonore, offers a strategic blueprint for how the United States, Europe/Germany, and African institutions (notably Africa CDC) can work collaboratively to secure the modern bioeconomy. It proceeds by outlining the current landscape of AI–biotech convergence, examining major threat vectors, proposing an integrated set of policy measures, and concluding with recommendations for immediate action.

The stakes are high and the April 16 panel discussion unambiguously summarized them as follows:

- Offensive cyber operations against bio-laboratories and AI systems can steal **dual-use knowledge**.
- **Commoditization of AI** significantly lowers the barrier for malicious actors. Tools once requiring supercomputers are now runnable on laptops, accelerating potential dual-use abuses in biotech.

- **Genomic data**—extremely valuable for healthcare, population-level analytics, and novel therapeutics—**can be weaponized** to target communities or undermine trust in medical systems.
- **Pervasive IP thefts occur** in highly sensitive biotech sectors, with a significant proportion of next-generation genomic equipment located in jurisdictions where data protection is dubious.
- **The quantum-computing race** is moving faster than expected and outpacing the adoption of quantum-resilient encryption to protect decades' worth of genomic data.
- **Fragmented regulations** often focus on the "how" rather than the "why," failing to align security-by-design with broader innovation goals.
- **Emerging bio-economies in Africa** and elsewhere could become **focal points of data exploitation** if they do not receive adequate support for cybersecurity and data governance.

Addressing these challenges requires a new paradigm—one that integrates cybersecurity with biosecurity under a single governance umbrella. This paper proposes key steps for policymakers, especially in the United States, Germany/Europe, and Africa CDC, to align and act.

1. The AI x Biotech Convergence: Transformative Potential Meets Vulnerability

The 21st-century bioeconomy—encompassing genomics, diagnostics, advanced manufacturing of biologics, and agricultural biotech—is being rapidly transformed by AI. This convergence is more than just an incremental shift in research capacity; it redefines who can do high-level biotechnology, how fast, and at what scale. At the same time, the digitization of biology and reliance on cloud-based platforms invite serious cybersecurity challenges.

AI accelerates drug discovery by generating candidate molecules in days rather than months. Robotics, laboratory automation, and cloud laboratories allow research teams to execute experimental workflows with minimal human intervention. Additive manufacturing (3D bioprinting) is emerging as a new mode of production for medicines and biologics. Meanwhile, genomic data from humans, animals, and pathogens increasingly powers AI-driven insights—ranging from patient-level diagnostics to nationwide pathogen surveillance.

Yet with the rapid convergence of AI and biotech comes the risk of digital attack. Cyberthreats can now target genomic data, reprogram automated laboratory systems, corrupt AI training datasets, or exfiltrate proprietary research for economic or military advantage. In a global context of systemic competition, particularly between the United States and China, converging technologies form an unprecedented attack surface.

Transformative Opportunities

AI systems have radically accelerated the pace of biosciences:

- **Automated Molecular Design**: Machine-learning and deep-learning models such as generative adversarial networks (GANs) or large language models (LLMs), adapted for protein and small-molecule design, can produce new molecular structures at scale.

- **Cloud Labs and Robotic Automation**: AI orchestrates complex experimental workflows, providing an "autonomous laboratory" model that can transform small biotech startups into lean R&D powerhouses.
- **Genomics at Scale**: Next-generation sequencers, some of which are portable and the size of a USB drive, feed large datasets into AI-driven analytics. This makes it possible to track viral, bacterial, and human genomic data in real time.

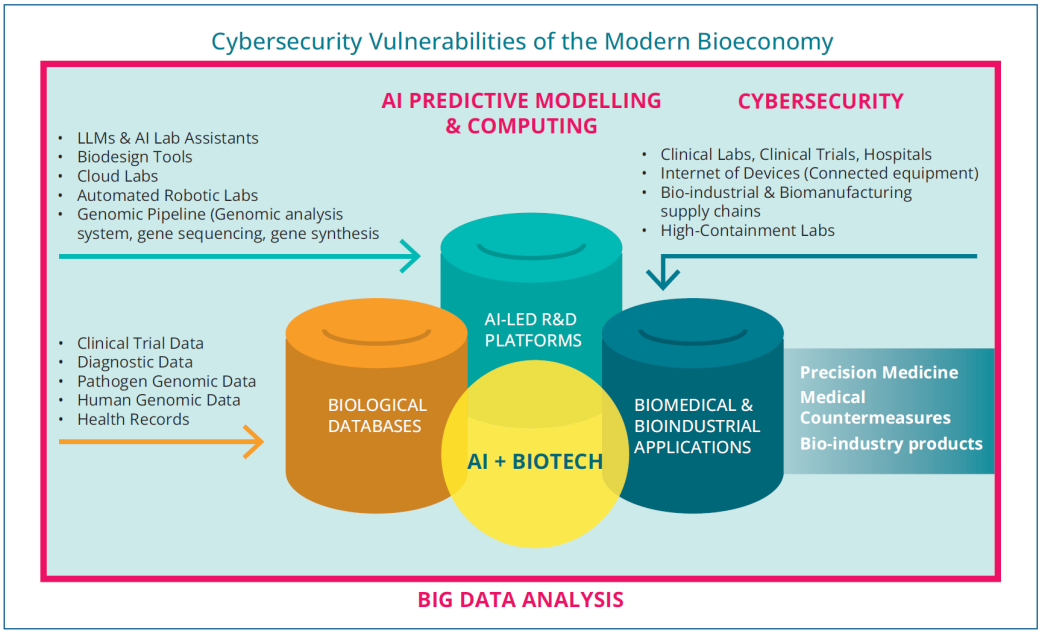
Equally significant is the "democratization" of biotech. Many emerging economies in Africa can leapfrog older sequencing technologies, directly adopting cutting-edge platforms. This yields massive potential for local innovation, public health benefits, and faster outbreak detection.

Heightened Vulnerabilities

Simultaneously, AI–biotech integration exposes multiple new threat vectors:

- **Data Integrity Attacks**
  - Poisoned datasets: AI models for precision medicine or pathogen identification can be surreptitiously fed corrupted training data, undermining therapeutics or diagnostics.
  - Manipulated genomic records: Attacks on genomic data repositories can degrade trust, hamper epidemiological investigations, or mislead research into developing the wrong treatments.
- **Infrastructure Takeover**
  - Hijacking cloud labs: Malicious actors can use compromised AI "lab assistants" to run dangerous experiments, produce toxins, or sabotage drug production.
  - Disruption of biomanufacturing: A ransomware attack on vaccine or insulin production lines can threaten national health security.
- **Dual-Use Knowledge Proliferation**
  - AI systems once needing supercomputers can now run on consumer-grade GPUs or laptops. Malicious actors can combine widely available software tools with stolen genomic datasets, designing harmful pathogens or toxic molecules at minimal cost.
  - Pathogen design: Generative AI models originally developed for drug discovery can be manipulated to design new toxic molecules or identify high-risk pathogens that might be synthesized.
  - Genetic subpopulation targeting: If adversaries gain access to large human genomic datasets, they may develop more precise—but ethically abhorrent—means of targeting specific ethnic groups.
- **Quantum Threat Horizon**
  - Policy discussions severely underestimate the quantum threat. Quantum computers, once fully operational, can break classical encryption—particularly if current data protection remains static.
  - Preparing for "post-quantum" security is not an abstract exercise; the data we fail to protect now will be decrypted later, exposing entire populations.

- **Fragmented Regulations and Rushed Adoption**
    - The U.S. often regulates technology in non-prescriptive ways, focusing on procedural compliance over outcome-based security. In the EU and Germany, layered regulations can slow adoption but also create blind spots where biotech does not integrate with national cybersecurity strategies.
    - Emerging economies in Africa leapfrog to cutting-edge genomics but often lack robust national policy infrastructures to ensure data integrity. Without urgent capacity-building, they risk exploitation.



2. Strategic Perspectives

United States: Innovation Hub with Fragmented Cyber Defenses

The U.S. leads in AI research, biotech startups, and genomics data collection. However, it struggles with a slow-moving regulatory apparatus and a mosaic of state- and federal-level cybersecurity standards. Efforts at CISA (Cybersecurity and Infrastructure Security Agency) have only recently begun to address the bioeconomy as critical infrastructure. The U.S. regulatory environment often focuses on *how* a technology is regulated rather than *what outcome* policymakers seek. Meanwhile, IP theft—particularly alleged large-scale data exfiltration by Chinese entities—continues to compromise the U.S. biotech sector.

Key needs in the U.S. context include:

- Upgrading oversight frameworks so that biotech R&D, big data, and AI governance align with cybersecurity demands.
- Establishing clearer lines of responsibility between federal agencies (e.g., FDA, NIH, DHS, and DOD) on bio-cyber incidents and response strategies.
- Integrating quantum-resilient encryption and molecular cryptographic methods into federal guidelines and NIST standards. While NIST has begun standardizing post-quantum algorithms, adoption across the biotech ecosystem is neither incentivized nor funded at scale.

Germany and the European Union: Between High Regulation and Accelerating Needs

Germany recognizes biotech as part of critical infrastructure essential for economic security and is simultaneously implementing the EU AI Act, GDPR, and other data-protection regimes. However, the existing frameworks are siloed, focusing on discrete sectors rather than the entire "DNA to AI pipeline." Germany aims for technological sovereignty but has not yet deeply integrated cybersecurity into policy for the bioeconomy. Policymakers must address how diverse regulations (data privacy, AI oversight, biosecurity laws) intersect and occasionally conflict.

Opportunities for Germany and the EU include:

- Developing a coherent "Security-by-Design" directive that applies to laboratory equipment, genomic data repositories, AI research, and biomanufacturing.
- Championing a new "data classification standard" for genomic information, thereby harmonizing sharing and privacy practices across EU member states.
- Supporting the formation of robust, multi-stakeholder consortia that can build upon and refine approaches like the BioISAC model in the United States.

Emerging Bio-economies in Africa: Leapfrogging with Security in Mind

Africa is rapidly acquiring state-of-the-art sequencing capacities and data systems—often skipping older technologies altogether. This *clean slate* environment offers a unique opportunity to embed cybersecurity in the genomic and AI infrastructure from the outset, but the ecosystem is not fully ready.

Many African nations need:

- Investing in critical AI-biotech infrastructure to secure data centers, ensure reliable encryption, and well-regulated cloud environments to handle sensitive genomic information.
- Building regulatory capacity (including national strategies that link AI, genomics and cybersecurity) and clear data-governance frameworks that allow for controlled sharing while respecting privacy and avoiding exploitation.
- Developing skills and foresight, including support for universities, research centers, and Africa CDC in training a new cadre of cybersecurity-savvy genomics professionals.

Because Africa's datasets are vital for global health research—including potential vaccines, treatments, and pathogen surveillance—there is a pressing need for equitable benefit-sharing agreements. Without strong cybersecurity and intellectual property protections, African nations may become mere data providers, ceding wealth and strategic advantage to external actors.

3. Policy Imperatives for Cyber-Biosecurity in the AI–Biotech Era

Drawing on expert insights shared by Sultan Meghji, Dr. Sterling Sawaya, and Dr. Sofonias Tessema, this section outlines four strategic imperatives to future-proof the convergence of AI and biotechnology.

Imperative 1 — Embed Security-by-Design in AI–Biotech Systems

The cyber protection of the bioeconomy must begin at the design stage.

- **Hardening Laboratory Devices:** Many gene sequencers and robotic lab platforms come from startups lacking embedded security. Regulators and consortia must establish baseline standards for firmware, wireless protocols, and data encryption.
- **Encrypting Genomic Data by Default:** Raw sequencing data should be encrypted at source, governed by strong key-management systems that remain under the data owner's jurisdiction.
- **Institutionalizing Red-Teaming:** AI-enabled biotech labs must undergo regular adversarial testing to uncover cyber–biosecurity vulnerabilities, especially in high-throughput automated environments.

Imperative 2 — Build Tiered Data Frameworks and Cryptographic Standards

Moving beyond the binary model of "open" or "closed" data access, we need structured data governance calibrated by risk.

- **Tiered Data Classification**
  - Tier 1: Low-risk aggregated genomes (e.g., bacterial reference libraries).
  - Tier 2: Moderately sensitive data (e.g., emergent viral strains).
  - Tier 3: High-sensitivity assets (e.g., human population genomics with metadata, or lethal pathogen blueprints).
- **Molecular Obfuscation Techniques**: Sequence-blending and molecular cryptography tools can preserve data utility while preventing re-synthesis of potential biothreats.
- **Post-Quantum Encryption**: Next, medium-term priority is to migrate genomic repositories to quantum-resilient cryptographic standards—future-proofing AI-enabled bio innovation.
- **Global Data-Sharing Platforms**: Secure-by-design architecture must underpin platforms like GISAID or GenBank. An improved interoperable system—co-led by Africa CDC, NIH, and European agencies—could enforce consent management, cryptographic tiering, and controlled access.

Imperative 3 — Forge Global and Regional Governance Coalitions

No single actor can manage the cyber–biosecurity frontier alone. We must catalyze collaboration:

- **Public–Private Partnerships** (PPPs): Just as PPPs guided the creation of the early internet, biotech–AI security demands PPPs with cloud providers, biotech startups, research labs, and standards bodies.
- **Regional Leadership**
  - U.S.: Expand NIST's and DARPA's mandates to cover bio–AI security standards; empower CISA to coordinate cyber–bio risk management.

  - Germany/EU: Lead a "Biotech Secure-by-Design" initiative akin to GDPR but cross-cutting through data, labs, and critical infrastructure.
  - Africa: Scale the Africa PGI as a governance anchor; fund genomics-AI cybersecurity pilots in local biotech hubs.
- **Global Forum**: Institutionalize AI–biotech governance through intergovernmental channels (BWC, WHO, NTI/IBBIS, etc.) to synchronize cyber risk policies, attribution protocols, and secure data standards.

Imperative 4 — Invest in Infrastructure and Capacity

Without foundational infrastructure and human capital, these strategies cannot scale:

- **Train a Cyber–Biosecurity Workforce**: Develop interdisciplinary curricula that merge genomics, AI, and cybersecurity—across universities, industry upskilling programs, and South–North academic partnerships.
- **Retrofit Legacy Infrastructure**: Harden existing sequencing labs with encrypted firmware, secure cloud pipelines, and real-time monitoring tools.
- **Enable Equitable Tech Transfer**: Empower labs in emerging bio-economies with access to encrypted equipment, secure servers, and funding mechanisms earmarked for cybersecurity and responsible innovation.

4. Recommendations

Policymakers need a clear, implementable roadmap. Below is a six-point action plan to operationalize the above imperatives over the next 12–18 months:

- **Establish National Cyber-Biotech Security Task Forces**
  Form interdisciplinary task forces—including genomics experts, cryptographers, cybersecurity analysts, and legal advisors—in the U.S., Germany, and across Africa (via Africa CDC). These teams could coordinate national strategies and multilateral engagement.
- **Launch a Secure Data Governance Pilot**
  Select 2–3 pathogens of regional concern (e.g., Ebola, flu variants, antimicrobial-resistant strains) to pilot a secure data classification and access protocol. Include AI labs, local health authorities, and cloud service providers.
- **Set Standards for Secure Sequencing Devices**
  Collaborate with biotech hardware manufacturers to develop and certify new sequencing machines with embedded encryption chips, secure firmware update protocols, tamper-resistant physical and digital logs.
- **Create Incentives for Secure-by-Design AI Tools**
  Offer fast-track regulatory approvals, innovation grants, or tax relief for biotech firms that demonstrate robust cyber architectures—e.g., AI pipelines with end-to-end encryption, bias detection, and adversarial robustness.
- **Mandate Post-Quantum Encryption for Biorepositories ?**
  Update national and international data storage protocols to mandate NIST-approved post-quantum encryption for high-risk genomic data. This protects against both present and future state-sponsored data exfiltration.

- **Stand Up a Global AI–Biotech Threat Observatory**
  Modeled on the BioISAC, this global observatory would 1) aggregate threat intel from national CSIRTs, biotech companies, and public health institutions; 2) monitor AI-assisted cyber intrusion attempts into genomic databases; 3) coordinate international response playbooks and rapid alert mechanisms.

5. Conclusion

The convergence of AI and biotechnology promises to reshape our world in ways scarcely imaginable a decade ago. Breakthroughs in precision medicine, pandemic preparedness, and sustainable manufacturing are within reach. Yet, without bold and coordinated action to secure these capabilities, we risk a future where malicious actors exploit genomic data, compromise medical supply chains, and even design dangerous biological agents with AI' support.

The stakes for national security, global public health, and economic stability are profound. The imperative—as Sultan, Sterling, and Dr. Tessema each underscored—must be to embed security at every layer, from the hardware of next-generation sequencers, to the AI systems that power automated labs, to the global agreements that govern the sharing and classification of genetic information. Robust cybersecurity is not a barrier to innovation; it is the very backbone that can ensure innovation proceeds safely, ethically, and at scale.

In practical terms, realizing a secure, equitable, and prosperous bioeconomy demands:

- Multilateral Coordination that respects national sovereignty yet converges around shared standards and a universal commitment to minimize dual-use risks.
- Expanded Funding for cyber–bio infrastructure, so that advanced nations and emerging bio-economies alike can protect genomic data while leveraging its potential.
- Forward-Looking Regulation that sets baseline security requirements, incentivizes security-by-design, and clarifies how to handle the most sensitive pathogen or population-level data.
- Inclusive Skill-Building to cultivate a global cadre of genomics professionals with expertise in cybersecurity, AI responsible innovation, and data governance.

None of this will be easy. But as the panel discussion emphasized, the AI–biotech revolution is already unfolding at breathtaking speed—and the window for proactive action is limited. Policy inertia, fragmented initiatives, and outdated legal frameworks will only widen vulnerabilities and allow adversaries to exploit them at scale. Instead, a strategic, well-funded, and globally coordinated effort can channel the transformative power of AI–biotech convergence—securing public health, bolstering economic resilience, and fostering trust in the next generation of biotechnological innovation.

The Author

Eleonore Pauwels is an international expert in the security, societal, and governance implications generated by the convergence of artificial intelligence with other dual-use technologies, including cybersecurity, genomics, and genome-editing. Pauwels provides expertise to the World Bank, the United Nations, and the Global Center on Cooperative Security in New York. She also works closely with governments and private sector actors on the changing nature of conflict, foresight, and global security, as well as responsible innovation related to Al, biotechnologies, and cybersecurity.

ln 2018 and 2019, Pauwels served as Research Fellow on Emerging Cybertechnologies for the United Nations University's Centre for Policy Research. At the Woodrow Wilson International Center for Scholars, she spent ten years within the Science and Technology Innovation Program, leading the Anticipatory Intelligence Lab. She is also part of the Scientific Committee of the International Association for Responsible Research and Innovation in Genome-Editing (ARRlGE). Pauwels is a former official of the European Commission's Directorate on Science, Economy and Society.

Pauwels regularly testifies before U.S. and European authorities including the U.S. Department of State, NAS, NIH, NCl, FDA, the National Intelligence Council, the European Commission, and the UN. She writes for *Nature, The New York Times, The Guardian, Scientific American, Le Monde, Slate, UN News, The UN Chronicle*, and The World Economic Forum.

Disclamer

Konrad-Adenauer-Stiftung e. V.

Konrad-Adenauer-Stiftung USA
1233 20th Street, NW, #610

Washington, DC 20036
USA

www.kas.de/usa