

BIOTHREAT ASSESSMENT 2035



Biothreat Assessment 2035

By

COL Dan Mitchell
COL Laura Porter
LTC Matt Rasmussen
LTC Timothy Harloff
LTC Justin De Armond

United States Army War College
Class of 2022

DISTRIBUTION STATEMENT: A

Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

About This Document

The United States Army War College (USAWC) student team BioThreat Forge prepared this document as an Integrated Research Project to complete the Strategic Research Requirement portion of the Master of Strategic Studies degree program. The research, analysis, and production of this report occurred from November 2021 through May 2022 in



conjunction with the resident Army War College Senior Service College curriculum. The team consisted of two U.S. Army Colonels (O-6) and three U.S. Army Lieutenant Colonels (O-5): Dan Mitchell (Special Forces), Laura Porter (Army Nurse Corps), Matt Rasmussen (Infantry), Timothy Harloff (Aviation), and Justin De Armond (Acquisition Corps), respectively. Team “Biothreat Forge” provided the results of this study to Mr. William Nelson, Deputy Assistant Secretary of the Army for Research and Technology (DASA (R&T)).

Requirement

This report answers the question posed by Mr. Jeffrey Singleton, Executive Director for Technology for DASA R&T (See Annex A):

What surprising biotech capabilities will potentially threaten U.S. people, infrastructure, and/or the military by 2035?

Team BioThreat Forge analyzed estimates from open-source information relevant to the biotechnology industry. The team produced the final report in multiple mediums including a PDF (primary), soft-bound book, and a PowerPoint presentation.

Analytic Confidence

The analytic confidence for the key findings is *moderate*. Individual reports contained within this product carry their own analytic confidence. The posed question was complex and the timeline to produce an answer was relatively short due to competing requirements of the USAWC core curriculum. Source availability was high while source reliability and corroboration were low to high depending on the specific topic. The analysts were not subject matter experts and some topics required extensive scientific knowledge to fully grasp. The analysts worked independently and collaboratively to answer the question.

They utilized a combination of structured analytic techniques including nominal group technique and network analysis. The team evaluated their analytic confidence using Peterson's Analytic Confidence Factors coupled with the Friedman Corollaries (See Annex B).

Words of Estimative Probability

Team BioThreat Forge utilized the Kesselman List of Estimative Words as their Words of Estimative Probability (WEP) for determining the likelihood of a biotechnology capability to threaten U.S. people, infrastructure, and/or the military by 2035 (See Annex C). Analysts used these WEPs in individual estimates of specific threat capabilities, as well as in the analysis of the biotechnology trends towards 2035.

Source Reliability

Analysts note source reliability at the end of each citation as low (L), moderate (M), or high (H). The citation was directly hyperlinked to the open-source content at the time the analyst produced the estimate. Team BioThreat Forge determined source reliability using the Standard Primary Credibility Scale and the Trust Scale and Website Evaluation Worksheet (See Annex D). Figures and photos embedded throughout this document are also hyperlinked to their source.



Daniel D. Mitchell

Daniel D. Mitchell

daniel.d.mitchell.mil@army.mil

Laura L. Porter

Laura L. Porter

laura.l.porter12.mil@army.mil

Matthew S. Rasmussen

Matthew S. Rasmussen

matthew.s.rasmussen.mil@army.mil

Timothy A. Harloff

Timothy A. Harloff

timothy.a.harloff.mil@army.mil

Justin L. DeArmond

Justin L. De Armond

justin.l.dearmond.mil@army.mil

Key Findings

It is highly likely (71-85%) that combinations of 13 key biotechnology capabilities will threaten U.S. people, infrastructure, and/or the military by 2035. This probability is a synthesis of individual capability estimates as shown in Figure 2. The team researched a larger number of biotech capabilities and trends and used analytic techniques to derive the most important capabilities and trends impacting the US by 2035. Team BioThreat Forge broke these capabilities down into **3 sets: Biotech, Biotech Related, and Biotech Enabling**. The first, **Biotech**, is a series of capabilities using organic material or its components to create a product or process, generally originating from genetic engineering and synthetic biology. The second, **Biotech Related**, is a series of capabilities comprised of hardware and software specifically designed to enhance research and development. The third, **Biotech Enabling**, are capabilities that originated outside of biotech but are increasingly important to the industry. These key capabilities arose from multiple sectors and are the major drivers of 5 interrelated trends that could generate threats by 2035.

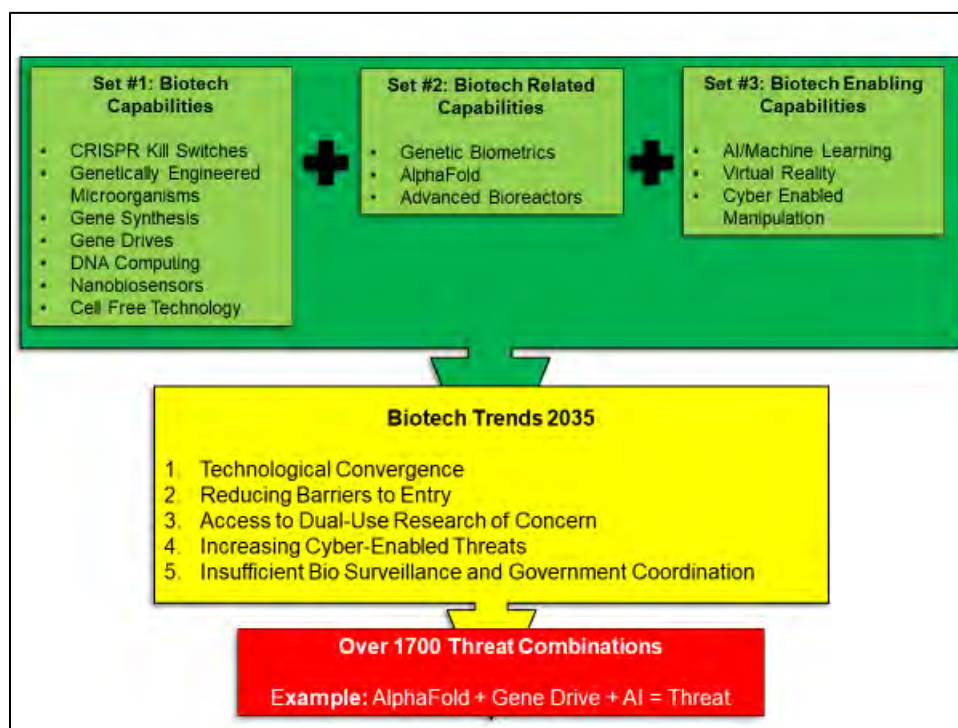


Figure 1 Key Findings.

Trend #1 is the convergence of digital technology, both hardware and software, which accelerates research and development. **Trend #2** is the reduction in barriers to entry to biotech through the diffusion of tools, techniques, and knowledge. **Trend #3** is access to unregulated dual-use research of concern (DURC) that allow many actors to use knowledge and potentially bioengineer threats. **Trend #4** is the increase of cyber-enabled threats and hacking that will disrupt research, development, production, and supply

chains. **Trend #5** is insufficient bio surveillance capability and government coordination for future public health crises.

Each of these 13 capabilities by itself are not necessarily threatening. However, when biotech capabilities are combined with each other, and with ill intent, the result then becomes a biotech threat. Using a Combination calculator, there are over 1700 combinations of these capabilities. Taken together with the 5 trends, these findings demonstrate how a combination of two or more of the 13 key capabilities can allow a state or non-state actor to engineer a significant number of threats to US people, infrastructure, and the military by 2035.

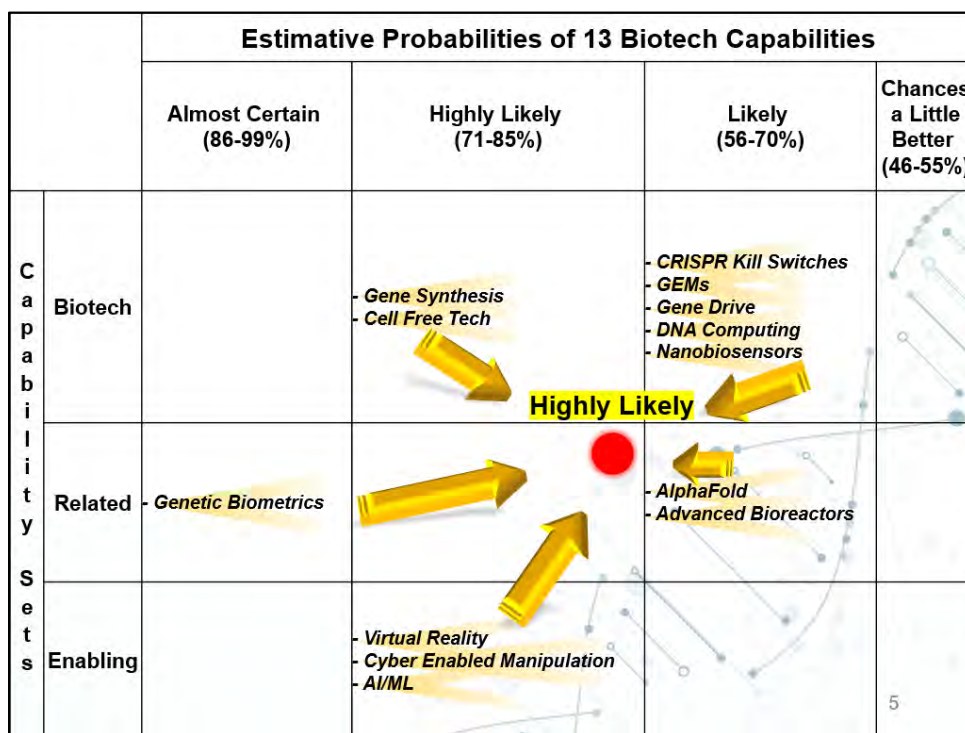


Figure 2 Individual Capability Estimates.

Trend #1: Technological Convergence

Technological convergence is advancing the pace and significance of biotech development in ways that are highly likely (71-85%) to produce surprising threats by 2035. Technologies such as **Artificial Intelligence/Machine Learning (AI/ML)**, advanced computer processing, nanotechnology, **Virtual Reality (VR)**, robotics, and autonomous systems are disrupting the biotech industry. The pace of convergence has accelerated in the last twenty years due to information proliferation and the global connection via the internet. Technology is allowing researchers, biologists, and entrepreneurs to use biotech to solve previously intractable problems using new technological developments. **AI-enabled** microbiology modeling, such as **AlphaFold**, and other elegant biological tools that tech advances enabled, such as CRISPR-Cas9, are

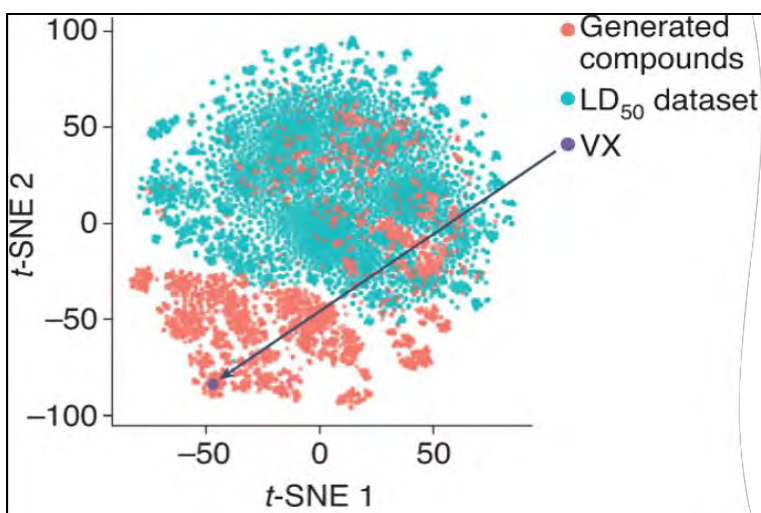


Figure 3 AI Generated Lethal Chemicals.

having outsized impact on biotech. *CBInsights*, a private equity research company, reports that **AI/ML** and robotics are in use to assist food production. **AI/ML** analyzes satellite imagery, conducts in-field monitoring, assesses crop and soil health to provide predictive analytics.

Research recently published in the *Nature Machine*

Intelligence Journal demonstrated the ability for **AI** to develop over 40,000 lethal chemical molecules in less than six hours with a tweak to an existing algorithm.

Biotech convergence is highly likely to solve the world's limitation on data storage due to a lack of silicon. **DNA computing** is highly likely to be a practical alternative to silicon-based circuits, providing increased storage and advanced computing power. *MIT's Technology Review* records that scientists first discovered **DNA computing** in 1994; but it is only in recent years that advances in computer processing have massively expanded the ability to manipulate DNA and cells in a way that enables bio-computing to become practical. Researchers estimate the data stored in the entire World Wide Web could be stored in a coffee cup of DNA material. Devasir Bennet from the *Center for Applied NanoBioscience and Medicine* at the University of Arizona published an article in the journal *Nano Select* in 2021 discussing techniques such as DNA nanoengineering, DNA origami, and enzymatic nicking which have made DNA computing and genetic manipulation more efficient.

Nanotechnology and biotech are converging to realize multiple uses in research and industry. **Nanobiosensors developed by Roswell Biotech**, can detect single virus particles like COVID-19 instantly or multiple times within seconds at ultra-low concentrations of a substance with an active electrical current. **Nanobiosensors** to detect pathogens show promising military applications as arrays of connected sensors deployed on mounted or dismounted equipment to detect pathogens.

Researchers are using **VR** to study complex biological structures that form the building blocks for all biotech applications. *Immersive Science* developed a tool called *ConfocalVR* that allows researchers "to visually step inside cells and see things they never saw in 2D." Employing similar technology, *Insilico Medicine* researchers used VR

in May 2020 to evaluate several COVID-19 protease inhibitor drug candidates in a simulated environment. It is likely that improved VR technologies will provide assistance to scientists in the development of more robust and resilient **genetically engineered microorganisms (GEMs)**.



Figure 4 Scientists Using VR to Evaluate COVID Drugs.

Gene sequencers and **gene synthesizers** dramatically increase the efficiency and quality of research by automating what was once time-consuming and monotonous labor for lab techs.

Technological convergence is producing tools and methods that delegate the non-creative repetitive work of bioscience to computers and machines, allowing humans to refocus on innovation and discovery to revolutionizing the biotech field.

Possible 2035 Threat Combination:

Scientists using Deep Mind's Automated Intelligence **AlphaFold** software and **virtual reality** can make exciting breakthroughs on proteomics, discovering new relationships between protein structure and enzyme function. Seeking to weaponize microbiology, a state military research laboratory uses these same tools to determine a short duration, nonlethal pathogen targeting common bacteria in the human gut biome. Using gene editing and **gene sequencers**, a State produces this pathogen in aerosol form, testing it a neighboring State's major metropolitan area.

Headline:

"Hundreds sickened by aerosol release in subway, officials say"

Trend #2: Reducing Barriers to Entry

Easier access to knowledge and lower costs required to develop biotech is highly likely (71-85%) to result in a non-state group producing a biological threat to the U.S. by 2035.

Competition in the biotech industry will spur innovation increasing the quality of goods while lowering costs. As access to more capable biological material and advanced equipment increases, traditional barriers to entry decrease and open the door for non-traditional actors to enter the biotech space. According to the *National Intelligence Council's Global Trends 2040* report, "Biotechnology is likely to make significant contributions to economic growth during the next two decades, potentially affecting 20% of global economic activity by 2040, notably in agriculture and manufacturing."

Increasing numbers of entrepreneurs and hobbyists are leveraging tools of the information age, such as YouTube and online forums, to share knowledge and materials. Among biotech companies are startups such as Josiah Zayner's *The Odin*, who have the express intent of "seeding the biohacking revolution." Anyone with a desire to learn can purchase genetic material and Do It Yourself (DIY) biotech kits



Schools are enhancing biology programs with genetic manipulation technologies from companies like *Amino Labs*, an online biology education and equipment company, giving children hands-on education in genetics.

Their website states their mission is to make “biotech learning and innovation accessible to everyone.” The

American Society of Cell Biology is advocating that high school biology programs need to do a better job incorporating genetics education. Other technologies like **VR** are enhancing learning

opportunities for aspiring

biotechnologists and reducing individual knowledge requirements. The Danish company *Labster* is using **VR** to create simulated laboratories for students to learn biotech methods using the latest equipment while reducing resource requirements. The company *BioBits* markets **Cell Free technology**, a rapid method for protein synthesis not requiring live cells. With it, high schools and others can conduct molecular biology experiments with minimal cost and equipment. These same technologies are almost certain to be used by independent nefarious actors and ill-disciplined hobbyists on a budget. Overall, barriers to practicing advanced microbiology and genetic manipulation are decreasing the entry level knowledge and funding required, which is highly likely to increase biotech threats to the U.S.

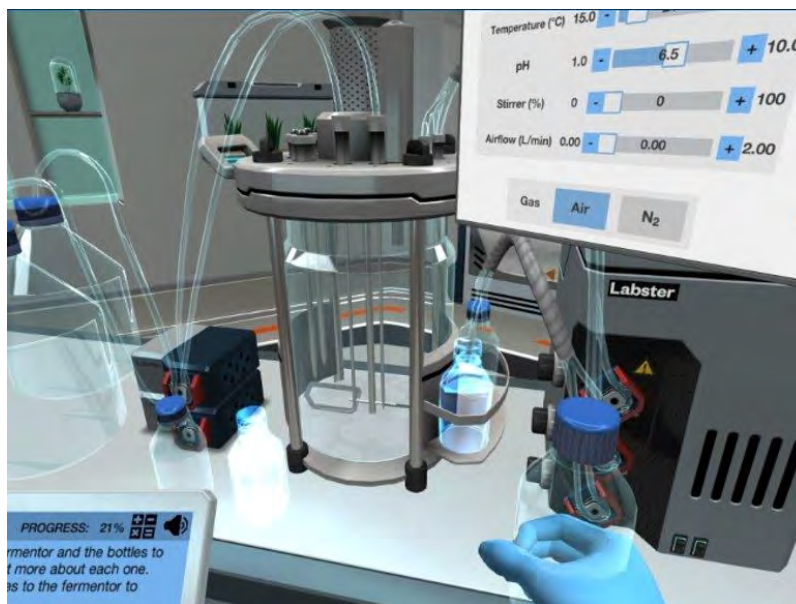


Figure 6 Virtual Lab from Labster.

Possible 2035 Threat Combination:

An aspiring biotechnologist uses an online biotech **virtual laboratory** to learn the basics of how to grow bacteria. They purchase an **advanced bioreactor** capable of automating the production and growth process under the guise of creating personalized medicine. They create a deadly bacterium in their garage. Due to a leak in the bioreactor, a household pet contracts a bacterial infection. The pet spreads it to other animals in the neighborhood through its feces resulting in hundreds of pet deaths.

Headline:

“Hundreds of local pets dead from homemade bacteria leak, spread to humans feared”

Trend #3: Access to Dual-Use Research of Concern

It is highly likely (71-85%) access to Dual-Use Research of Concern (DURC) will contribute to the development of a significant threat to the U.S. by 2035. *The National Institute of Health* defines DURC as the misuse of science to adversely threaten humans, animals, plant life, industry, the environment, or national security. Team BioThreat Forge’s research discovered the concept of “Dual Use” has a wide and varied interpretation. Academia and science typically associate Dual-Use with ethical misuse, such as using CRISPR to genetically modify human embryos. The military tends to view dual use as the weaponization of a technology. Most scientists in the biotech industry do not typically associate their research with weaponization, rather they view their work altruistically. It is significantly concerning that most countries are either unaware of the risks or place little emphasis on Dual-Use ethic and that others are actively trying to weaponize biotech.

A Pakistani study of postgraduate research students published in the journal Health Security in 2019 showed 76.7% of respondents had never heard of DURC or were unsure of its meaning. Additional research by Svenja Vinke and the *Carnegie Endowment for International Peace* supported the transferability of these findings. Research methods and biosecurity measures have shown wide disparity globally. The *John Hopkins Center for Health Security* and the *Nuclear Threat Initiative* ranked China and India among the worst in the 2021 *Global Health Index* with the lowest score possible in precautions for

Dual-Use research and creating a culture of responsible science. Unfortunately, no country in the report showed improvement from the previous year in this area.

China and other adversaries will likely use recent advances in

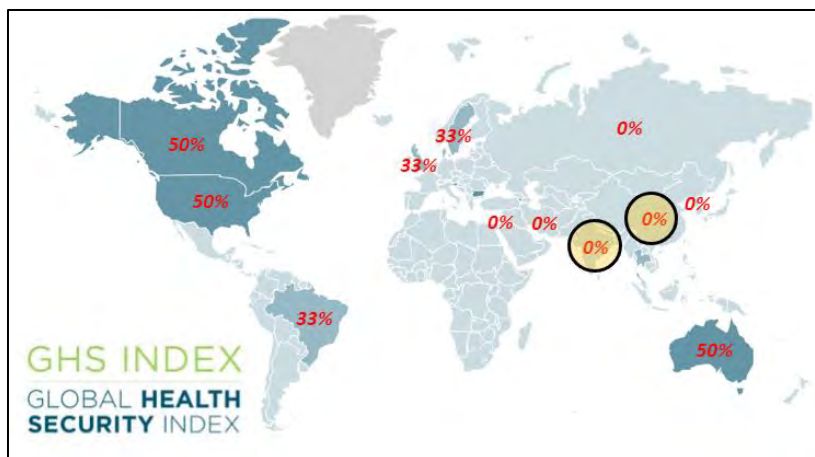


Figure 7 Global Health Index in Precautions for Dual-Use Research.

genetics for Dual-Use applications, and in some cases have expressly stated they intend to weaponize these discoveries. China's two most recent Five-Year Plans indicate biotech is a prime priority for development. A paper published by Colonel Guo Ji-wei in *Military Review* outlines the Peoples Liberation Army's (PLA) view on the military applications of biotech, mentioning the weaponization of protein structures or proteomics to precisely target specific populations. According to the journal *Nature AlphaFold*, an AI protein-modeling tool, is a leap forward in proteomics that is highly likely to help the Chinese realize their goal. In 2019, Defense One assessed other Chinese publications detailing PLA research into the military application of gene editing which indicates China's view of biotech as a new military domain. **Gene drive** is one such technology that China could weaponize. Researchers at the *Wyss Institute for Bioengineering* at Harvard University have demonstrated the **Gene drive** process where scientists preference the selection of

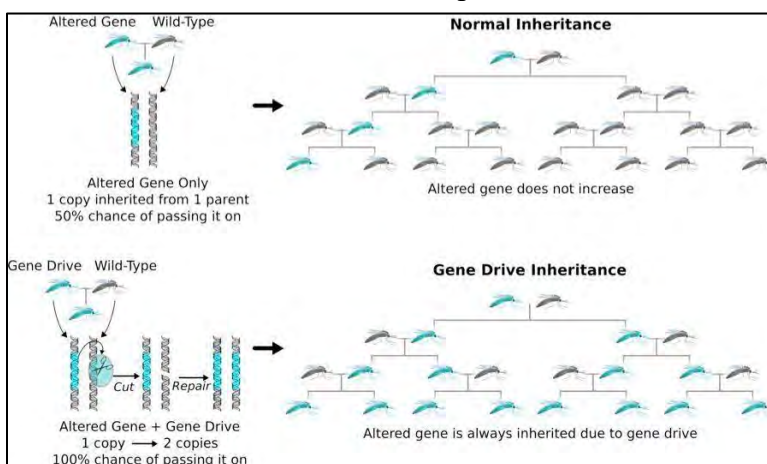


Figure 8 Gene Drive Process.

one parent's genetic trait over the other's, replacing natural selection. Wyss Researchers postulate that **Gene drives** can confer sensitivity to a specific chemical, environmental particle, or prodrug that could be activated later within a confined geography or population.

Another significant advancement in **Genetically Engineered Microorganisms (GEMs)** is the development of **CRISPR-Cas9 Kill Switches**, as published in *Nature Communications*. The research shows these **Kill Switches** allow programming of microorganisms to activate, deactivate, or eliminate themselves. A state unconstrained by ethics could harm a rival's bioeconomy

by weaponizing **Kill Switches** to attack good bacteria that prevent disease or pathogens then shut off or die before spreading uncontrollably.

In many ways the focus on scientific discovery and knowledge is outpacing the legal, ethical, policy, and regulatory environment. Mr. Daniel Gerstein, Former Deputy Under Secretary for Science and Technology at the Department of Homeland Security, has written that international agreements on bioweapons and bio-ethics are insufficient and dated. The U.N. acknowledges there is no international regulatory agency with sufficient authority to do more than investigate the post-facto use of a suspected biological weapon, and even then, there is little consequence for their use.

Possible 2035 Threat Combination:

Ethnically homogenous states seeking to protect their culture emphasize research into what makes a person ethnically similar. Upon discovering this genetic similarity, they use **Gene Drive** to impart immunity to diseases and pathogens, connecting this immunity to their distinct ethnic gene. They then create a pathogen their ethnic population has immunity to and release it in major population centers after testing.

Headline:

“Ethnic cleansing made possible by “gene bomb” that targets genetic differences, officials say”

Trend #4: Increasing Cyber-Enabled Threats

It is highly likely (71-85%) that Cyber enabled threats will increasingly allow malicious actors to steal biological research, corrupt data, emplace malware, and attack hardware by 2035. The extreme reliance of biotech on a digital

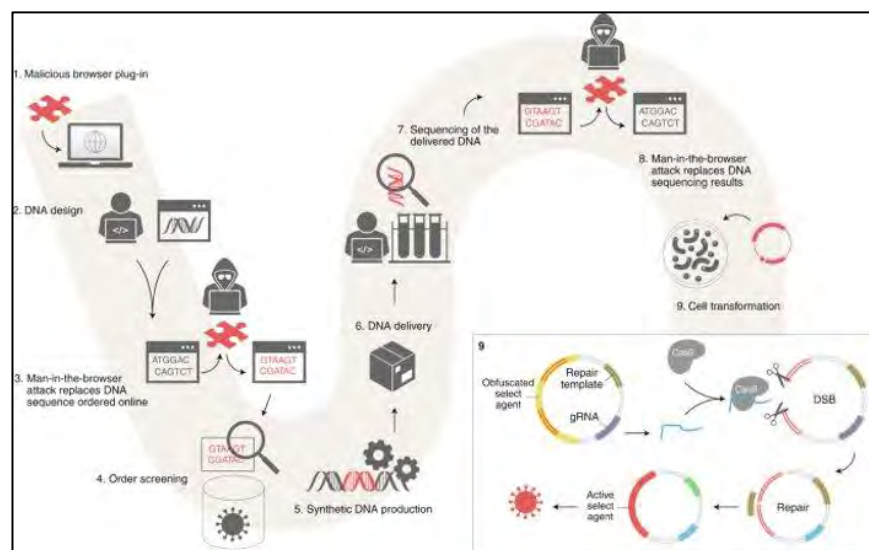


Figure 9 Cyber Attack to Create Toxic DNA.

backbone brought about by convergence creates new vulnerabilities for adversaries to exploit. These threats are aimed at corrupting digital and physical genomes, disturbing computer systems, networks, data storage, and process control, and disrupting biotech workflows and supply chains. The *European Centre of Excellence for Countering Hybrid Threats* identified similar cyber-enabled threats. Hackers can manipulate and corrupt biomedical research datasets or manipulate the functioning of deep-learning analysis systems. Researchers at Yale and Ben-Gurion University in Israel have demonstrated how hackers can penetrate synthetic biology databases to place malicious code or toxic strands into mapped DNA sequences. This cyber-enabled manipulation makes synthetically engineered DNA toxic to the recipient.

The conditions of the COVID-19 Pandemic have given cyber-attackers experience to improve their techniques with a massive increase in cyberattacks throughout 2020. These more experienced cyber attackers will continue to press their advantages and shift focus to more complex targets. In the spring and fall of 2021, biomanufacturing firms in the US were hit by a malware called “Tardigrade.” This “metamorphic” malware system acts autonomously to hide inside computer systems and funnel data without external control. Non-state actors are responsible for this most recent increase in cyber-attacks. However, FBI warnings from 2021, and the US Intelligence Community 2022 *Annual Threat Assessment*, point to China, Russia, and Iran as additional cyber threats to US digital infrastructure.

Cyber-attacks on health care institutions are at an all-time high, according to *Critical Insights*, a cybersecurity company. Hackers target the medical industry to steal or ransom data at an average \$7 million dollars per incident according to *Fierce Healthcare*. Theft of this information could not only delay delivery of life saving services, but has the potential of providing hackers necessary information to target specific individuals.

Cyber-hacking is almost certain (86-99%) to enable domestic surveillance in authoritarian states such as China. **Genetic Biometrics** is using DNA as a tool to reliably identify a person in addition to other characteristics such as fingerprints, retinas, and facial structure. **Genetic Biometrics** is also the only tool that allows security officials to determine familial relationships. Authoritarian states could use this to target family members of dissidents or foreign officials. Adversary states could correlate **Genetic Biometric** information with other PII, obtained by cyber-hacks such as the OPM, Anthem Health, or Equifax breaches to target American government officials via espionage or blackmail. Should the Chinese successfully hack the Armed Forces DNA Identification Laboratory (AFMES-AFDIL) they could correlate the DNA information of Service Members from the past 50 years with other stolen data. The *Beijing Genomics Institute* works hand-and-hand with the PLA and is building the largest DNA database in

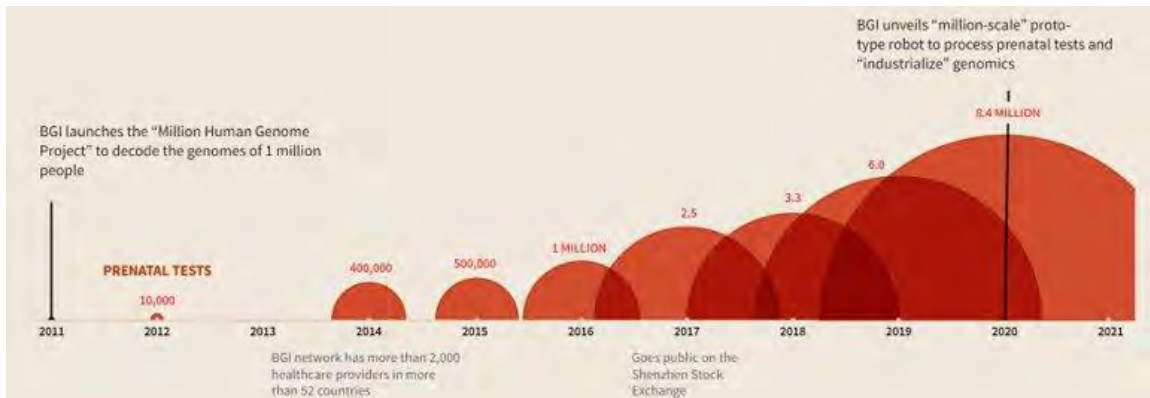


Figure 10 Beijing Genomics Institute DNA Collection.

the world, which currently houses over 140 million samples. It is likely that future foreign customs agencies will require DNA sampling and verification using rapid **Gene Sequencers** putting U.S. Intelligence, Diplomatic, and high value individuals at risk.

Barring a massive unforeseen change in the use of computers, AI, and digitization in modern biotech research and industry, cyber-enabled threats will continue to grow in importance to biotech.

Possible 2035 Threat Combination:

Hackers attack a biotech data bank housing food data sets and change the **DNA sequence** just enough to remain below the level of monitoring software. The corrupt DNA sequence is used by a bioreactor to manufacture food which is now tainted.

Headline:

"Hackers sicken thousands with tainted yogurt at Fort Hood"

Trend #5: Insufficient Government Coordination and Bio Surveillance

Insufficient bio surveillance and lack of government coordination make it highly likely (71-85%) the US will not be able to effectively respond to a significant public health crisis by 2035. The *Interim National Security Strategic Guidance* has clearly put forth the concept that biological threats are national security concerns. threats as a national security concern. The COVID-19 pandemic has provided a play book for bad actors on how to destabilize political and societal infrastructure. Microbiology researchers from Southern Illinois University believe it is just a matter of time before a bioterrorist uses a sizeable bacterial attack to inflict "widespread damage." Key to protecting the population from natural or synthetically developed pathogens is the ability to detect and respond quickly.

Bio surveillance is a complex, multi-domain system comprised of active and passive modes. Active surveillance is done via random field sampling and patient laboratory testing results. Passive surveillance is comprised of health information data and social media reports. Warning systems to ensure safety and security of the public are not currently sufficient. In 2021, the Office of the Inspector General identified that the Department of Homeland Security's *Bio-Watch* sensor system has severely limited capabilities in air and water quality detection and is inadequate to the task. The *Roswell nanobiosensor* technology is a solution that is likely to provide rapid, cheap, and accurate methods to quickly determine and decipher threats.

Without implementing changes to address BioWatch's challenges, the United States' ability to prepare for, detect and respond to a potential bioterrorism attack is impeded which could result in significant loss of human life.

- Source: OIG-21-22



Figure 11 BioWatch Sensor System.

Lack of consistency in focus and funding allows biotech capabilities to become greater threats to public health. A report by *Trust for America's Health* (TFAH), a non-profit/non-partisan public health advocacy group describes this trend. The U.S. government and populace gives temporary attention to public health investment during crises, but then moves to other priorities when the emergency passes. TFAH states this “boom-bust cycle has left the nation’s public health infrastructure on a weak footing.” Funding levels for public health initiatives, in-

cluding surveillance measures, have decreased over the last two decades. The *Robert Wood Johnson Foundation* has identified the U.S. public currently lacks “trust or confidence in key public health institutions necessary to address current or future challenges.” Multiple studies and reports, including the *World Economic Forum* study on Public-Private Cooperation on Pandemics, have indicated a factor leading to distrust is inequality and lack of cooperation between entities. In a 2021 book chapter *Coordination of Public Health Response: The Role of Leadership in Response*, LTG(R) Russel Honoré, who led military relief efforts post Hurricane Katrina, validates this conclusion, stating public health failures are due to a lack of effective coordination and collaboration between local, state, regional, and national public health systems. While acknowledging the overall importance of medical surveillance systems, the military intelligence system defers to outside civilian entities to provide this capability. When asked regarding the integration of

bio surveillance into the military intelligence community, a senior leader indicated this was not an Army mission. Synchronized government surveillance and response to public health is instrumental in providing the monitoring, analysis and action plans necessary for protection from biological threats. Without it, the biotech capabilities discussed in these findings become even more threatening.

Possible 2035 Threat Combination:

State public health officials over the past five months identified an unusual amount of people seeking medical care, but laboratories have been unable to definitively determine a causative agent. Experts are suspicious the symptoms are from an emerging organism and are working to develop testing methods to identify it. Most victims are requiring hospitalization, and bed space and supplies to support them are running at critical lows. The Centers for Disease Control is collaborating with State authorities to assist with organism identification and determine why **information systems** did not identify the trend sooner to alert officials. Seven months after the event it was determined a terrorist organization, Red Dawn, introduced a pathogen known to be highly contagious via respiratory transmission to destabilize the population leading up to a planned election.

Headline:

“Mystery illness overwhelm hospitals, impact upcoming election”

Table of Contents

| | |
|--|-----------|
| About This Document | 1 |
| Key Findings..... | 4 |
| Analytic Reports Supporting Key Findings..... | 19 |
| Genetics Advancements Supercharged By Technology Convergence Highly Likely To Create Greater Threats By 2035..... | 20 |
| Artificial Intelligence (AI), Nanotechnology, and CRISPR Kill Switches Likely to Accelerate Biotech Threats by 2035 | 23 |
| Reducing Barriers To Entry Highly Likely To Attract Non-Traditional Actors To Biotechnology By 2035 | 26 |
| Bio-Convergence Highly Likely to Create Threats And Opportunities For Industry And Government By 2035..... | 30 |
| Unanticipated Medical Biotech Threats Highly Likely In The Future | 33 |
| Engineered Microbes Likely Attack Crops and Die Afterwards by 2035 | 36 |
| Bacteria Use Likely In The Next Biological Attack From Now To 2035..... | 38 |
| Genetic Synthesizer Advances Highly Likely To Proliferate DNA Editing Technology To The Masses By 2035 | 41 |
| Gene Drive Technology Likely To Increase Risk Of Genetic Based Threats By 2035 | 43 |
| DNA Computing And Genetic Circuits Likely To Have Military Use By 2035 | 45 |
| Nanobiosensors Protecting Food Security Likely Within Ten Years | 48 |
| Cell Free Technology Highly Likely To Be A Bioweapon By 2032..... | 50 |
| Enzymes Capable Of Rapidly Degrading Common Plastics Highly Likely By 2035.... | 52 |
| Advanced Bioreactors Likely Available To The General Consumer By 2035..... | 55 |
| Deep Mind's AlphaFold Likely To Have Weaponizable Dual Use For Proteins, Enzymes And Toxins | 57 |
| China Almost Certain to Use Genetics as a Part of Surveillance by 2025 That Threatens U.S. Security and Economic Prosperity..... | 59 |
| Weaponized Artificial Intelligence and Blockchain Highly Likely to Threaten Agriculture in Ten Years | 61 |
| Cyberbiosecurity Highly Likely To Be A Significant Driver Of Defense And Industry Spending By 2035 | 64 |
| Virtual Reality Highly Likely To Increase Access To Biotechnology By 2035..... | 67 |
| Additional Findings..... | 70 |
| China's Genomic Research Likely to Exceed U.S. by 2035 Enabled by Massive Collection of Human DNA Samples | 71 |

| | |
|---|-----------|
| Malicious Actors Likely To Utilize Public Health Threats For Global Bioterrorism Within 5-7 Years | 73 |
| Security Standards In India Make High Risk Biosafety Labs Risky | 75 |
| Medical Implanted Devices Pose Chance of Cyber Security Threat..... | 77 |
| Public Health Surveillance Systems Still Not Adequate by 2035 | 79 |
| Rapid Tech And Organization Changes Mean Algae Will Likely Be Major Source Of Food By 2035 | 82 |
| Another Pandemic Likely By 2035, But Not Due To Accidental Lab Release | 84 |
| Advances In Marine Biotech Will Make Weaponized Algae and Toxins Possible, But Unlikely, By 2035 | 87 |
| U.S. Highly Likely To Maintain A Competitive Advantage In Biotechnology Through 2035 | 90 |
| Nanomaterials Highly Likely to Increase Food Production Over the Next Decade | 93 |
| Biosurfactants Likely to Reduce Threats and Improve Biosecurity By 2035 | 96 |
| Annexes | 99 |
| Annex A – Terms of Reference | 100 |
| Annex B – Assessing Analytic Confidence | 104 |
| Annex C – Kesselman List of Estimative Words | 105 |
| Annex D – Source Reliability | 106 |
| Annex E – Interview/Communication Notes | 108 |
| Annex F – Briefing Slides..... | 125 |

Analytic Reports Supporting Key Findings



Genetics Advancements Supercharged By Technology Convergence Highly Likely To Create Greater Threats By 2035

Executive Summary

Technology convergence with genetics is highly likely (71-86%) to make biotech more available to all actors globally. Several key microbiology advancements produced paradigm shifts especially in genetics. Despite the benefits of advanced knowledge, these advancements are likely (56-70%) to pose military and non-military threats to the U.S.

Discussion

Technology convergence is accelerating the pace and significance of biotechnology advancements that are increasing the importance of biotech to national security. Three developments in the past ten years resulted in microbiology paradigm shifts particularly in genetic research and application. Advanced computing power, data science and Artificial



Figure 1 YouTube Video Demonstrating AI and Biotechnology.^M

Intelligence (AI), additive manufacturing, cyber, global connection through the internet and several other 21st century technologies made these breakthroughs possible.

Discovery of CRISPR-CAS9 in 2012 by 2020 Nobel Prize winner Jennifer Doudna, PhD,^M Deep Mind's AlphaFold protein shape prediction software in 2018,^H and the SARS-COV-2 (COVID) global pandemic that brought increased demand and proof of concept to gene sequencers,^{M,H} mRNA vaccines, and targeted drug development have had an outsized impact on genetics and microbiology.

Rapid advancements in genetic research and technology are gaining the attention of both nation-states and non-state actors. As biotechnology improves, the educational and financial barriers to entry decrease.^M Genetics is still exceptionally complex and requires extensive knowledge, expertise and funding to fully leverage; however, it is likely that many of these barriers will be much lower by 2035 based on the pace of advancements today.

The U.S. reigns supreme in biotechnology; however, China is an increasingly close second player.^H China's publications, research, and investment indicate intent to overtake

the U.S. by 2050. China's 13th and 14th Five Year Plans both indicate the priority they're placing on biotechnology.^{[H](#)^{[H](#)}} Additionally, Colonel Guo Ji-wei of The People's Liberation Army (PLA) and biotechnology writer and lecturer Xue-sen Yang outlined China's views military application of biotechnology and bioweapons.^{[H](#)} Guo and Yang specifically mention the weaponization of Proteomics to precisely target specific populations; AlphaFold is a leap forward in the study of protein structures and function that is highly likely to help the Chinese realize their goal.^{[H](#)} Other recent publicans detail PLA research into and the military application of gene editing, AI, and human performance that suggests China embraces biotech as useful military weapons and possibly a military warfare domain.^{[M](#)}

China's collection of vast amounts of genetic data from both their people and around the world reinforces their genetic research priority.^{[M](#)} Beijing Genomics Institute (BGI) is building the largest gene bank in the world, storing over 100 million human, plant and animal DNA samples.^{[H](#)} It is likely that this will enable Chinese researchers, using advanced computing and AI, to unlock increasingly more insights into the human genome and the specific functions of different segments.^{[M](#)} Since 2012, CRISPR-CAS9 has provided and elegant tool for modifying the genome to make use of the current



Figure 2 YouTube Video on How China May Lead the Bio-Revolution.^{[M](#)}

knowledge to modify biological organisms to cure disease, repair damaged segments, or provide enhancements such as HIV resistance.^{[H](#)} Once Chinese scientists understand how to modify the human genome to increase speed, strength, intelligence, immunity, and pathogen resistance they will likely use CRISPR to pursue their national interests.^{[H](#)}

BGI collaborates with the PLA and their gene bank likely serves a security purpose -- genetically enabled surveillance.^{[M](#)^{[H](#)}} The PLA and Chinese police forces have collected samples from ethnic minorities as well as dissidents, students, transients, and anyone else they determine to be a possible security threat.^{[M](#)} The Chinese police in Xianjian and other areas purchased gene sequencers and additional lab equipment that enable them to do in house DNA evaluation likely for identification purpose.^{[M](#)} China likely can correlate the DNA data warehoused at BGI with data stolen from various cyberattacks, such as the 2014 OPM breach, to their economic and security benefit and the U.S.'s detriment.^{[M](#)^{[H](#)}}

Genetic biotech advancements have placed tools in the hands of non-state groups such as corporations and hobbyist geneticists. It is possible to outfit a home lab for less than \$1000, and acquire CRISPR kits for less than \$200 through the internet.^H Gene sequencers have push button simplicity, provide near instantaneous results and are available for under \$1000.^H Publicly available gene synthesizers can build a DNA strand from raw materials that are available online or in the wild.^H Online DNA databases are unclassified *recipes* for biologicals to include viruses and bacteria.^H Indeed, schools are enhancing their biology programs with some of these materials and giving children hands-on education in genetics.^{H,M,H} All the tools, ingredients, and instructions are available to the hobbyist or the low-funded nefarious non-state actor.



Figure 3 YouTube Video on DIY Biohacking with The Odin.^M

Technology convergence has accelerated genetic research and lowered start-up cost for translating theory into application. While this allows the non-state actor access to leverage genetics for nefarious purpose, the U.S. DoD should be concerned about nation-states leveraging genetic for malign intent. China is developing greater capability and signaled their intent to use biotech as for national security.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst has no specialized microbiology education or training, worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Daniel D. Mitchell

Artificial Intelligence (AI), Nanotechnology, and CRISPR Kill Switches Likely to Accelerate Biotech Threats by 2035

Executive Summary

The convergence of AI, nanos, and CRISPRs are likely (56-70%) to supercharge biotech fields and increase threats due to its dual-use capability requiring new detection systems. Researchers and private industry are blending technology capabilities to enhance biotech despite the relative immaturity of integrating other technologies. AI combined with CRISPRs will generate new biotech opportunities and threats at increasing speed. The need for traditional and biological sensors will increase to defend against potential biohazards and quickly inform of immediate dangers. Utilizing new biotech techniques from nanos or CRISPRs to neutralize hazards to food security and other industries will enable swift responses to crises. Understanding and detecting novel biotechnology threats combined with AIs' ability to generate solutions in 2-3 years instead of 5-10 years requires a vigilant defense posture from weaponized biotech. [M](#)

Discussion

Merging innovative technologies like nanotechnology with biotech will likely accelerate the industries' growth and impact on the global economy and bring significant dual-use opportunities and threats (see Figure 1). The National Institute of Health defines

the dual-use research of concern capability covering the misuse of science to adversely threaten humans, animals, plant life, industry, the environment, or national security. [H](#)

Weaponizing AI and using adversaries' remote AI systems are likely to impact all aspects of biotech, including food security, in the next decade. [M](#) The US and our adversaries will use AI, machine learning, and robotics to assist all biotech industries by analyzing satellite imagery, environmental monitoring, predictive analytics, and autonomous

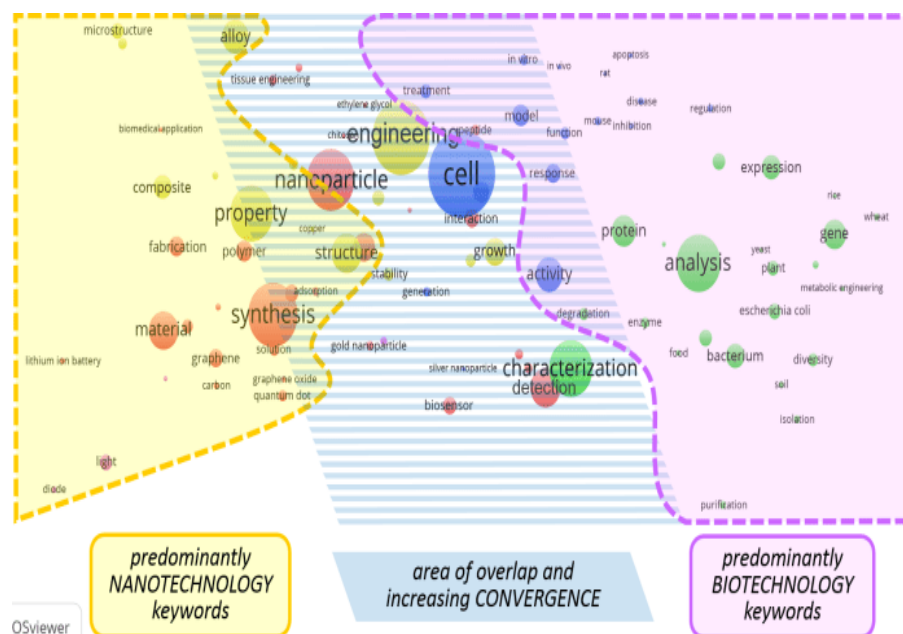


Figure 1 Overview of Nanotechnology Impacting Biotechnology. [M](#)

machines. [M.H.H](#) Other nations might use AI to weaponize algae's cyanobacteria and develop more lethal bioproducts impacting humans and the environment. [H.M](#) The government and industry must ensure the security of AI applications to deter adversaries as they look for dual-use biotech opportunities to impact food security, the military, and other US industries. Competitors are unlikely to follow international norms regarding responsible innovation. The cyber, digital, and physical monitoring systems we develop to protect the US must be flexible and fast to detect threats.

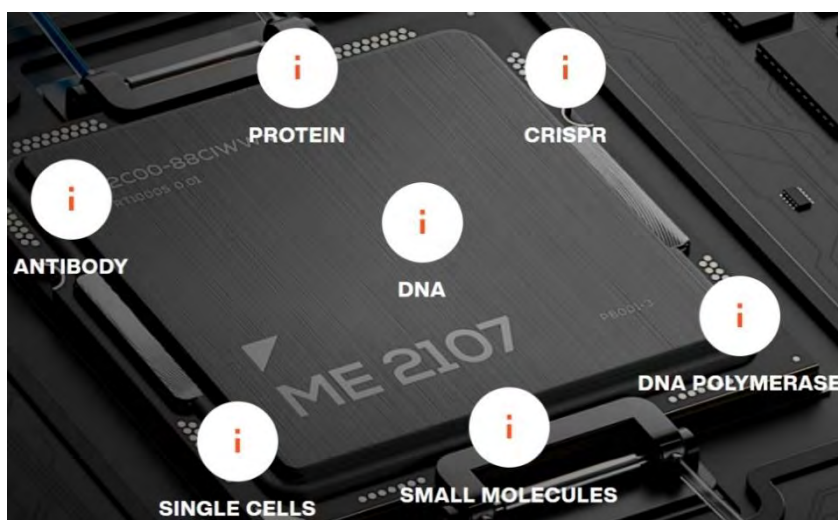


Figure 2 Roswell BioTechs Molecular Electronic Sensor Hazard Detection Capabilities. [M](#)

As China and other competitors develop dual-use biotech threats, there is an emerging need to monitor the food supply chain and other industries to reduce microbial threats requiring new methods of detection. [H](#) Despite current biosensor technology and antiquated monitoring systems

like ProMED, innovative companies are likely to bring nanobiosensor technology to the forefront to improve security across multiple industries. [H](#) Biosensor technology will go from reactive and expensive detection techniques to rapid, cheap, and accurate methods to quickly determine and decipher threats to national security. Advances using silicon nanowire field-effect transistors, graphene field-effect transistors, single-walled carbon nanotube-based that fluoresce in near-infrared, biological field-effect devices, and complementary metal-oxide-semiconductor technologies will improve the accuracy in detecting harmful pathogens and toxins in real-time, where some might be developed by US enemies'. [M.H.H](#)

Nanotechnology integrated into biotech provides many opportunities and poses potential threats to multiple industrial sectors. Despite the early development of nanos and unknown environmental impacts, including toxicity, continued research will lead to the commercialization of nanos in biotech and other industries. Developing nanos for agriculture using silica nanoparticles and carbon-based nanomaterials can also influence medical, industrial, military, and aquatic biotech areas. Enemies might utilize nanos to develop means to deliver pathogens, toxins, or create toxicity impacting the environment,

humans, or industry. Knowing more about how nanos interact with the living and non-living substances is imperative to detect and protect national interests.

China and other adversaries will likely use recent advances in genetically engineered microbes (GEMs) to find dual-use applications. A possible threat in GEMs is the development of Clustered Regularly Interspaces Short Palindromic Repeats associated protein 9 (CRISPR-Cas9)-based kill switches (CRISPRks) (See Figure 3).^H

CRISPRks eliminate antibiotics for efficient killing, where humans control what the microbes do and then make them disappear.^H

Competitors might develop

CRISPRks to attack healthy bacteria preventing disease and other pathogens, negatively impacting the medical, agricultural, and other biotech fields and industries including the military. Exploiting predatory bacteria that hunt pathogens or CRISPRks GEMs are likely to help eliminate unwanted germs causing disease in many biotech fields.^M The US's enemies might use CRISPRks and other GEMs as a method of attack.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to how fast biotech is changing.

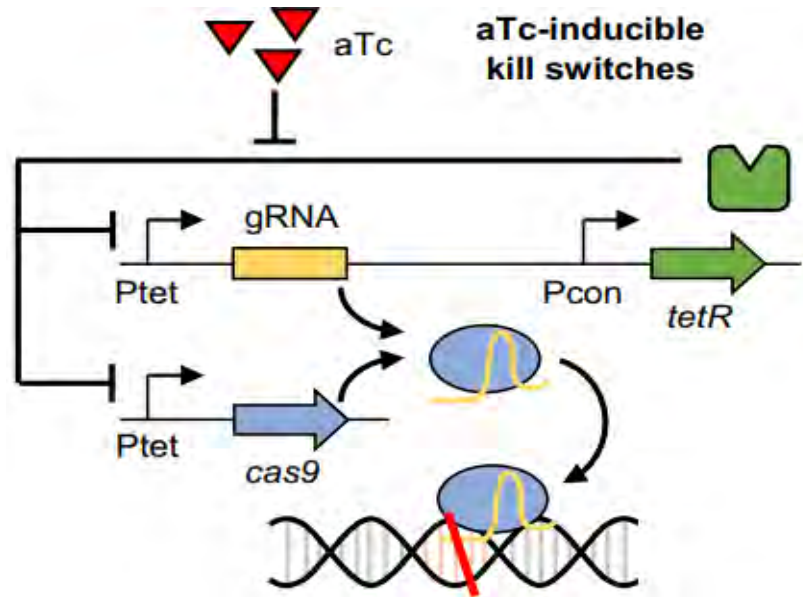


Figure 3 "In the presence of aTc, TetR is unable to bind to its target promoters, leading to expression of Cas9 and the gRNAs. The Cas9/gRNA complex then binds to and cleaves its genomic targets, leading to cell death."^M

Author: Justin L. De Armond

Reducing Barriers To Entry Highly Likely To Attract Non-Traditional Actors To Biotechnology By 2035

Executive Summary

Despite current high costs, required scientific expertise, and heavy resource requirements, reducing barriers to entry are highly likely (71-85%) to attract non-traditional actors to biotechnology by 2035. The biotechnology market continues to grow at a rapid pace spurring innovation and lowering prices. Virtual Reality and other technologies create new learning opportunities for aspiring biotechnologists while reducing individual knowledge requirements. Access to more capable biological material and advanced equipment is increasing. As traditional barriers to entry continue to reduce, the door opens for non-traditional actors to enter the biotechnology space with the potential to exploit the dual nature of this technology.

Discussion

Commanding a huge market cap, biotechnology continues to permeate several areas within industry “including biopharma, industrial, agricultural, food, environmental, and bioinformatics.”^M As of 21 March 2022, the top 376 publicly traded biotechnology companies in the world carried a market cap of over \$4.9 trillion.^M High value and high quantity of companies in the industry signals plenty of competition, which “basic economic theory demonstrates...leads to lower prices, higher quality goods and services, greater variety, and more innovation.”^M Despite downturns in the biotechnology market in 2021 and a series of layoffs across the industry in early 2022, investors are still demonstrating a “strengthening...appetite” for what many still think is an undervalued sector.^{M.M} As the economy continues to recover from COVID-19, many investors expect biotechnology to outperform the rest of the market due to its high level of innovation and continued public investment.^M Demonstrating this confidence, venture capital fund 5AM Ventures just closed two new biotechnology funds valued at \$750 million “suggest[ing] investments in biotechs aren’t going anywhere anytime soon.”^M As innovation in the biotechnology market expands, so does the access to information and education.

In a field of study that is notoriously difficult to learn, advancements in Virtual Reality (VR) are showing the potential to “offer new entry points to learners” and expand knowledge for current practitioners.^M The Danish company Labster is using VR to create simulated laboratories for students to learn biotechnology methods using the latest equipment while reducing resource requirements(See Figure 1).^M Additionally, researchers are using VR to study complex biological structures that form the building blocks for all biotechnology applications. The company Immersive Science developed one such tool called ConfocalVR that allows researchers “to visually step inside...cells

and see the things they never saw in 2D”.^M Employing similar technology, researchers used VR in May 2020 to evaluate several COVID-19 protease inhibitor drug candidates in a simulated environment.^H VR offers a safe and inexpensive method to experiment with biotechnology illustrating the potential for novices to access the field of biotechnology and experiment without traditional scientific expertise.

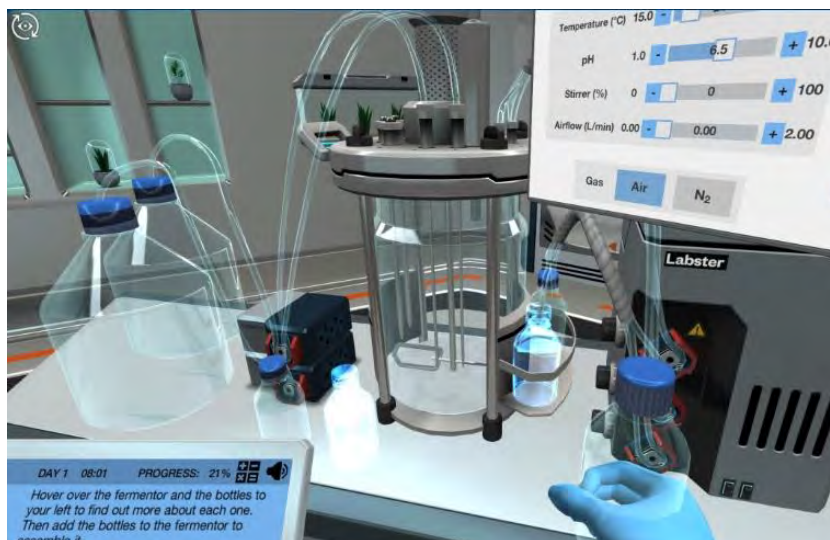


Figure 1 Example of a Simulated Lab from Labster.^M

Artificial Intelligence (AI) offers another potential avenue to lower the personal knowledge required to operate in this space. Although not biotechnology directly, researchers recently demonstrated the ability for AI to develop over 40,000 lethal chemical molecules in less than six hours with a simple tweak to an existing algorithm.^M It is a logical leap to assume a similar process could be employed in the biological space, further reducing barriers to entry. While biotechnology innovation and access to education is on the rise, the tools of the trade are also improving.

Bioreactors, which are known as “the backbone of the bioprocessing industry” are showing significant signs of advancement and increased access for the general consumer.^H What was traditionally a stainless steel or even a single-use vessel used to induce biochemical processes are being completely redesigned. Scientists are outfitting bioreactors with smart sensors and actuators while augmenting the control process with AI and cloud computing to increase efficiency, robustness, and lower overall cost.^H Additionally, tissue engineers are adding scaffolds and biosensors inside bioreactors to create 3D cell structures and monitor cellular activity allowing greater control over the process.^H Even today, there is wide access to bioreactors. As an example, the company Biorealize manufactures bioreactors for the general consumer advertising “tools and platforms that make it easy to do biodesign.”^M It is likely that this trend will continue with each technology iteration becoming more advanced and easier to employ.

Biomaterials themselves are also improving with the help of mother nature and synthetic biologists. In a 2021 study, researchers discovered over 30,000 non-redundant enzymes in nature exhibiting the ability to degrade common plastics.^H More importantly, scientists demonstrated the synergistic potential of enzymes in 2020 by combining two enzymes together to degrade a plastic bottle six times faster than a single enzyme.^H Additionally, synthetic biologists have demonstrated the ability to improve the robustness of bacteria by adding protein reserves to the bacteria allowing it to survive in harsh environments.^H More recently, researchers from Osaka University in Japan published a study on 11 April 2022 illustrating their ability to engineer bacteria to use light for energy allowing the organism to use more of its cellular resources to conduct chemical synthesis.^M Additionally, the Korean Advanced Institute of Science and Technology (KAIST) published a new method on 4 March 2022 combining Raman spectroscopy and machine learning to identify bacteria from environmental samples quickly and with a high level of accuracy.^M Engineered biomaterials coupled with the ability to easily pull these organisms from nature illustrates the increasing access to more capable organisms for use by biotechnologists and non-traditional actors.

Translating the potential of this changing biotechnology landscape to actual nefarious activity by non-traditional actors is difficult to predict. While it might be an easier task to determine the motivation for a large actor like the Chinese People's Liberation Army who broadcast their desire to exploit the offensive capabilities of biotechnology, non-traditional actors remain hidden from sight.^M

What is problematic is that the expanding pool of do-it-

yourself biotechnologists who can “build a fully functional genetic engineering lab at home by spending as little as \$1,000 on eBay” or less.^M Within the crowd of biotechnology companies are startups like *The Odin* who have the express intent of “seeding the biohacking revolution.”^M Anyone with a desire to learn can purchase genetic material and a slew of DIY biotechnology kits to include a \$169 Bacterial Gene Engineering CRISPR kit (See Figure 2).^M And as seen during the COVID-19 pandemic, DIYers were actively attempting to produce a vaccine and this trend is increasing.^M



Figure 2 A \$169 DIY Bacterial Gene Engineering CRISPR Kit.^M

Additionally, globalization and foreign investment creates a real opportunity for intellectual property exploitation with no guarantee how far or wide sensitive information spreads.^M Researchers are also battling with the issues of transparency versus security, noting that “open science” practices increase the risks of intentional or accidental use of biotechnology.^H Given these factors and the lack of a mitigation strategy, biotechnology advancement will present a significant challenge for national defense officials and this expanding threat space will require continuous scanning.

Characteristics of the changing biotechnology landscape are increasing innovation due to a growing biotechnology market, new entry points for education, widening access to resources, and an expanding pool of DIYers. These factors reduce barriers to entry and make it highly likely (71-85%) to attract non-traditional actors to biotechnology by 2035. This combination of people, equipment, and training plus intent will increase the possibility for non-traditional actors to employ this dual use technology in an unpredictable and harmful manner.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time, but the synthesis of information from multiple smaller research efforts made the task complex. The reliability of sources available varied, with the majority being above average. The sources available did corroborate each other and analyst collaboration was modest.

Author: Timothy A. Harloff

Bio-Convergence Highly Likely to Create Threats And Opportunities For Industry And Government By 2035

Executive Summary

It is highly likely (71-85%) that biotechnology will produce significant energy and food resources, resulting in increased threat of attack through cyber enabled methods. Due to anticipated scarcity of resources worldwide and increased interest in biotechnology caused by the COVID-19 pandemic, as well as the digital revolution and 4th Industrial revolution, technological and process efficiencies will be realized and will speed biotechnological research and advances. Resource scarcity issues will lead to more appealing incentive structures to drive industry to make more bioengineered solutions. The resulting massive reliance on digital systems and architecture in biotechnology research, development, and production creates multiple vulnerabilities which malicious actors can exploit, forcing industry and government to invest in greater cyber protection.

Discussion

Multiple forecasts of the future (2035 to 2050) describe a world where climate change and scarcity of resources affecting the “Water-Energy-Food” nexus that will drive

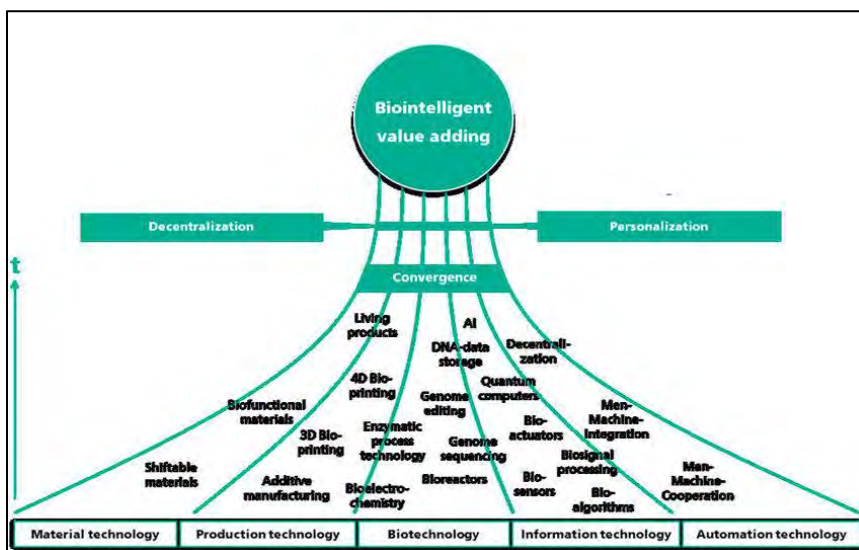


Figure 1 Graphical Representation of Bio-Convergence Creating Value and Incentive for Industry and Government.^M

opportunities, marine biotechnological research has lagged behind other biotech research and development. The COVID-19 pandemic both increased interest in biotechnology worldwide during the search for vaccines as well as caused significant disruptions in industry, production, and supply chains.^H Related to issues caused by the pandemic, but also due to continued advances in software and engineering, technological convergence is changing industry technology and processes to gain efficiencies and increase profit.^{H,M} Figure 1 graphically illustrates the types of technologies that are intersecting to accelerate

increasing human insecurity.^{H,H} Marine biotechnology has long held potential solutions to scarcity issues in these resource areas through the production of food, creation of bio-fuels, and ability to purify water.^{H,H,H} Despite the potential of these

research and development. Thus, it is highly likely (71-85%) that the convergence of multiple technologies, increased biotech research, and greater incentives for industry and governments to invest in cheaper and locally produced scarce resources will lead to marine biotech to be a major source of food, water, and energy.^M

The extreme reliance of an enlarged and expanded biotechnology industrial base on a digital backbone brought about by convergence creates new vulnerabilities that adversaries and enemies can exploit.^H As bioengineered materials are used more and more frequently, the biotech research, production, and supply chain is vulnerable at multiple points. Malicious actors can hack into and manipulate DNA catalogues and databases during biological research.^{M,H} Hackers can manipulate the programs and machines used in the production of biological material to taint products.^M With increased

access of the average person to synthetic biology materials, stolen data from biotech research could be used to bioengineer methods to attack food and water resources or kill people.^{M,M,M}

Figure 2 demonstrates examples of cyberbio threats and risks derived from bio-convergence.^H

| | | Convergent Risk Scenario | | |
|-----------------|--------------|--|---|--|
| | | In Silico Design of a Pathogen | In Silico Synthesis of a Pathogen | Brain-Computer Interface Exploitation |
| Risk Assessment | Probability | Adversary | Nation state, nonstate group, or individual | Nation state, nonstate group or individual |
| | | Timeline | Near term (0 to 5 years) | Mid term (6 to 10 years) |
| | | Democratization | Moderate | High |
| | | Vulnerabilities | Open access data, open source software | Limited customer verification |
| | | Needed scientific expertise and skills | Synthetic biology, genomics, bioinformatics | Synthetic biology, bioinformatics |
| | | Governability | Low | Moderate |
| | Consequences | Magnitude of potential consequences to economies, political systems, society, health, environment, and agriculture | Moderate | High |
| | | Sufficient existing countermeasures | None | None |
| | Risk | | Moderate | Moderate |
| | | | | |

Figure 2 Biotechnological Convergence Risk Assessment Framework Adapted from AAAS-FBI-UNICI, NASEM, and Tucker Frameworks.^M

The conditions of the COVID-19 Pandemic have already given cyber-attackers fertile experience. The spread of cyberattacks on biotechnological research and industry and specifically targeted cyberbiosecurity threats in 2021 demonstrate it is highly likely (71-85%) that cyberbiosecurity will be a major area of risk in the future.^{H,M} Multiple academic and industry sources are already advocating for more government regulation on cyberbio laws, regulations, and protections.^{M,H,H,M} The continuing severity and growing recognition of the cyberbiosecurity threat is highly likely (71-85%) to create pressure on industry, academia, and government to dedicate more resources to cyberbiosecurity measures.^H

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple academic resources confirm the ability and interest for increased marine biotechnological research towards practical application, however, it is not fully clear if the incentive structures will exist to push these advances towards wide acceptance by industry or the general population. The risks posed by cyberattacks to biotech industry are already a fact. It is clear that as with most biotechnological innovation, the synthetic biology means to engineer positive changes could be reversed to be negative or deadly. There was adequate time to complete the estimate, however the analyst worked alone with a general lack of expertise. The lengthy time frame of the estimate means the report is sensitive to change based off factors such as climate changes, population and migration movements, and economic shifts in the agricultural and industrial base.

Author: Matthew S. Rasmussen

Unanticipated Medical Biotech Threats Highly Likely In The Future

Executive Summary

Biotechnology is almost certain (86-99%) to have the capability to improve quality of life by 2035, reducing not only disease and hunger, but also improving manufacturing and fuel dependence. Industry projections indicate centering around economic growth, and research support this rapidly increasing trend. This trend while beneficial is not without its consequences. The negative impact of unregulated medical research, increased cyber security issues, high potential for pathogen manipulation, and lacking public health capabilities make it highly likely (71-85%) that medical threats related to biotechnology will not be anticipated.

Discussion

The biosecurity and research industry often discuss the concept of Dual Use Research of Concern (DURC). However, knowledge gaps persist. A Pakistan study of postgraduate research students showed 76.7% of respondents had never heard of DURC or were unsure of its meaning.^H Additional studies supported the transferability of these findings

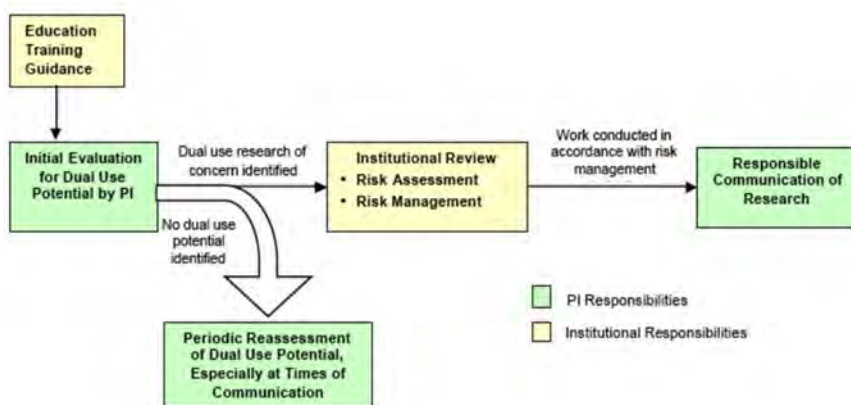


Figure 1 Steps in Local Oversight of Dual-Use Research.^M

second. In establishing a culture of responsible science, no country showed improvement from the previous year in this area.^H To avoid bio-risks posed by natural or synthetic biology, it is recommended those working with pathogens be adequately trained and work under strict management and regulation.^H Security and regulatory practices within the research community have shown significant diversity in understanding and advancement, which is a substantial area of concern.

Although the United States ranked highest in biosecurity safety standards according to the GHI, there remains a lack of mechanisms to standardize the reporting of biological incidents or exposures.^{M,H} “Without a standardized, international framework for reporting

laboratory incidents and responses, the task of mitigating such risks is difficult.”^M “Outside of the United States, the robustness of biosafety oversight varies significantly from country to country and region to region.”^H Countries like India are promoting laboratory and research facilities to grow the biotech industry for economic gain.^{M,H,H} Without any standardized global regulation or enforcement, safety and security practices are only voluntary and pose significant variability.^{H,H} This lack of enforcement capability was witnessed during the COVID-19 pandemic when Chinese authorities refused admittance of investigators to the facilities in question investigating the origin of the disease.^H

The risk expands when factoring in the Do-It-Yourself community. "Bacteria, mycobacteria, and viruses are prone to genetic manipulation," and evidence of this capability outside of regulated laboratories goes back to 2002 and is not isolated.^M Advancing technology has made the capability to acquire the infrastructure required to manufacture or manipulate pathogens out of a lab obtainable and affordable.^M “Since these groups often have limited formal training on the safety and ethics of using biotechnology, it might be difficult to contain and mitigate the impact of any accidents that may emerge from their experiments. Even though no unfortunate incident has happened so far, the absence of regulations to monitor this community has emerged as another safety threat.”^H

The cyber security market was increasing rapidly and expected to exceed \$376B by 2029,

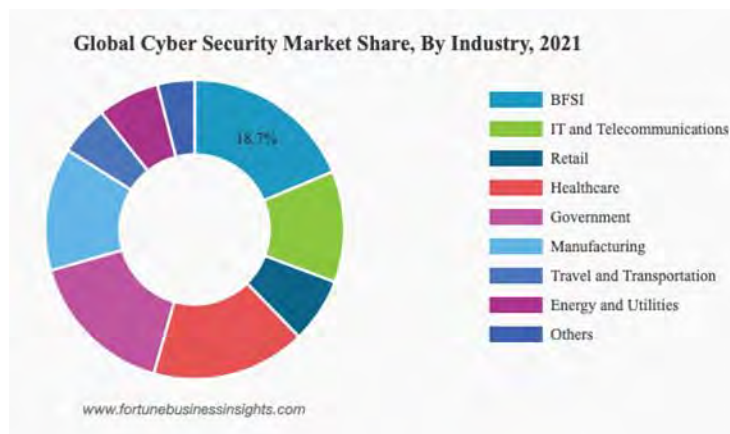


Figure 2 Global Cyber Security Market Share by Industry.^M

with healthcare expected to experience considerable growth.^M It is expected due to reliance on technology for nearly all aspects of life, nefarious actors will utilize the cyber domain as a targeting source.^M The medical community has experienced this as evidenced by unauthorized access to data, health information held for ransom, and concern

medical devices will be compromised.^{H,M} Ransomware payouts doubled between 2019 and 2020, costing the industry \$20.8B.^M The impact extends beyond a financial with “nearly a quarter of healthcare providers report increased mortality rates following ransomware attacks.”^M

Many factors comprise the concept of public health from a biosecurity perspective. Post COVID-19, Americans indicated the importance of a robust public health system with strong favorability to increase funding. However, historically, funding has been reduced significantly when the most previous public health crisis waned from public memory.^{H,H} This funding supports research in disease and subsequent treatments and delivers critical surveillance systems to identify emerging bioterror events or pandemics.^{H,H} This is not unique to the U.S., with “most countries seeing little to no improvement in maintaining a robust, capable, and accessible health system for outbreak detection and response, with 178 countries scoring less than 50% for the whole of government biosecurity systems.”^H

Artificial intelligence is rapidly expanding into the healthcare platform to improve healthcare delivery and assist public health surveillance.^{H,M} Active and passive surveillance systems have been constrained, making it challenging to utilize obtained data effectively long term due to but not limited to resourcing, legal/ethical, and technical

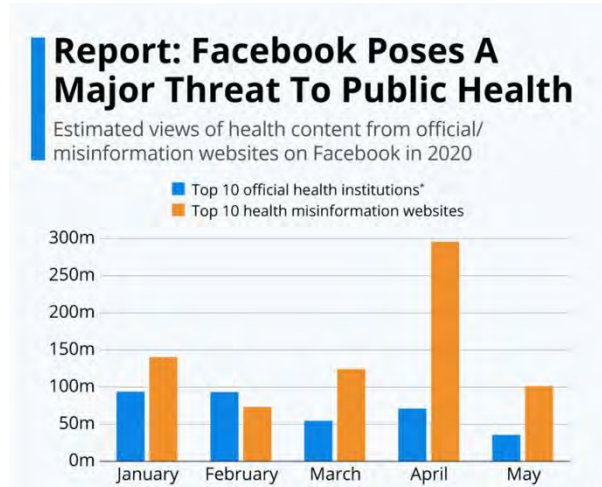


Figure 3 Misinformation on Facebook.^M

capabilities.^{M,H,H,H} Public opinion or mis/disinformation campaigns related to public health information is a key constraint.^{H,H} If information communication is not trusted or manipulated by outside sources, it can allow for vulnerability to be exploited by malicious actors.^{H,H}

Biotech offers the potential to improve the lives of the global population in many ways. However, the vulnerabilities offer a high potentiality

for exploitation by nefarious actors. Of the various domains (i.e., medical, industrial, etc.), negative medical or health care biotech implications impart a substantial risk to the population's welfare. Bad actors can, and it's highly likely they will, capitalize on the public fear and societal/political instability it can create.^{H,H}

Analytic Confidence

The analytic confidence for this estimate is high. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Engineered Microbes Likely Attack Crops and Die Afterwards by 2035

Executive Summary

Recent advances in genetically engineered microbes (GEMs) and the prospect of use in sustainable agriculture make it likely (56-70%) that the commercialization of GEMs will occur by 2035. Even though this biotechnology is in its infancy, start-up firms are likely to exploit genetic kill switches to control microbes that terminate their own life as helpful for the environmental bioremediation of toxins and other pathogens in sustainable agriculture. Additionally, this biotechnology will positively impact medical, industrial, and aquatic biotech. Adversaries could utilize this biotechnology to reengineer plant growth-promoting rhizobacteria (PGPR) and other bacteria to attack healthy biomes, jeopardize food security, and develop other offensive uses for attacking the US military.

Discussion

Since the advent of genetic engineering by biochemists Herbert Boyer and Stanley Cohen, scientists have continued to find novel applications for microbes.^H GEMs are entering a new era, and adversaries may utilize GEMs to disrupt competitors across multiple biotech fields. Additionally, the scientific consensus on the use of pesticides and antibiotics on crops depicts the harm to humans, animals, insects, and the environment.^{H,H,M} Of importance is the development of Clustered Regularly Interspaces Short Palindromic Repeats associated protein 9 (CRISPR-Cas9)-based kill switches (CRISPRks) (See Figure 1).^H

In 2021, scientists developed four CRISPRks that controlled and killed the target bacteria inside and outside the host.^H Kill switch activators are essential as the world is ever more integrating GEMs into the environment.^H Building stable kill switches into microbes used in agriculture could “kill pathogens that are deadly to crops.”^H This biotechnology allows

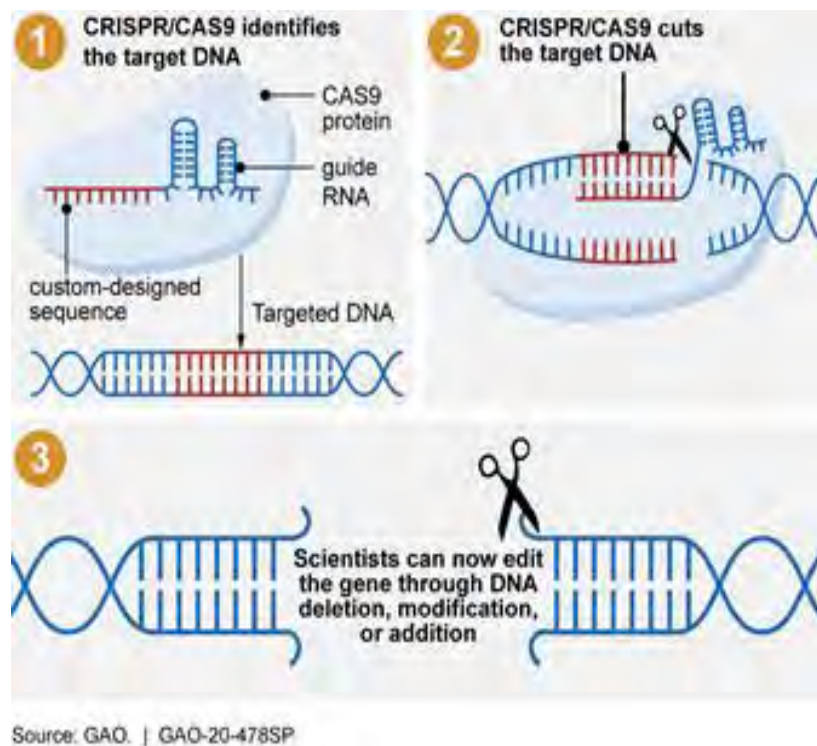


Figure 1 How the CRISPR-Cas9 Process Works.^M

for the elimination of antibiotics for efficient killing, where humans control what the microbes do and then make them disappear based on their CRISPRs design.^H At the opposite end of the spectrum, competitors might develop CRISPRs to attack healthy bacteria preventing disease and other pathogens from impacting the agro-economy.

Other research areas likely to benefit from CRISPRs are developing bacteria that eat other bacteria, removing antibiotics from agricultural processes and further developing PGPR. First, finding the most impactful predatory bacteria that hunt pathogens in the agricultural spectrum will help eliminate unwanted germs causing disease in crops.^M “Deployed under the right circumstances, they could help people beat back harmful microbes in the environment or purge pathogens from the food supply.”^M Integrating the CRISPRs into predatory bacteria might efficiently remove harmful pathogens and then remove themselves from impacting other organisms.

Second, as traditional antibiotics are harming bees and the balance in nature, CRISPRs, along with antisense antibiotics that utilize peptide nucleic acids (PNAs) conjugated to cell-penetrating peptides (CCPs) can inhibit targeted genes and stop the reproduction of the unwanted bacteria.^{H,H} This capability likely has dual-use purposes where an enemy develops methods to stop plant diseases and kill healthy bacteria if the proper PNAs target beneficial bacteria.

Lastly, genetically engineered PGPRs are healthy bacteria that improve the soil.^H In combination with “engineered strains of nitrogen-fixing soil bacterium *Azotobacter vinelandii* to produce ammonia and excrete it at high concentrations, transferring it into crop plants in lieu of conventional chemical fertilizers,” makes it likely to improve sustainable agriculture and reduce waterway contamination.^{H,H}

US adversaries are likely to utilize CRISPRs and other GEMs to develop ways to impact their opponents negatively. Targeting GEMs in the food chain and animal and human disease vectors are cause for concern, and competitors may develop CRISPRs that adversely impact healthy bacteria. Although not yet mainstream, dozens of start-ups, such as Hudson River Biotechnology and SNIPR Biome, are leading in the CRISPR field.^M With the new CRISPRs innovation, start-ups will likely start incorporating this biotechnology into their future commercial services.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to how fast biotechnology is changing.

Author: Justin L. De Armond

Bacteria Use Likely In The Next Biological Attack From Now To 2035

Executive Summary

Despite continuous efforts to sense and treat bacterial infections, it is likely (56-70%) bacteria will be the pathogen of choice in the next biological attack from now through 2035. Increased access, advancements in bacterium survival, and ease of employment make bacteria an easy choice for bioterrorists or Nations desiring to inflict casualties or reduce an adversary's available combat power.

Discussion

In 2001, one of the worst biological attacks in the history of the United States occurred. [M](#) Dr. Bruce Irvins, an Army biologist, mailed several letters to media outlets and two senators laced with deadly anthrax. [M](#) Five people died and 17 others became ill when they inhaled the bacteria, demonstrating how easily a nefarious actor could deliver a bacterial pathogen to a targeted audience with devastating effects. [M](#)

Bacterium, single-cell organisms, are “the most common and numerous organisms on the planet.” [M.M](#) In fact, there are an estimated 5 million trillion trillion (5×10 to the 30th power) on earth. [M](#) Obviously, not all bacteria are harmful or cause sickness. As an example, the human body contains an estimated equal ratio of bacteria cells to human cells (1:1) a lot of which are beneficial. [M.M](#)

However, there are plenty of harmful bacteria in the environment that pose a “global problem.” [M](#) As such, the World Health Organization (WHO) published a list in 2017 of 12 known families of bacteria that presented “the greatest threat to human health” due to their antibiotic resistance and their ability to “cause severe and often deadly infections.” [M](#)

Biotechnologists can pull harmful bacteria from the environment with ease and recent developments make this process even easier. On 4 March 2022, the Korean Advanced Institute of Science and Technology (KAIST) published a study citing their ability

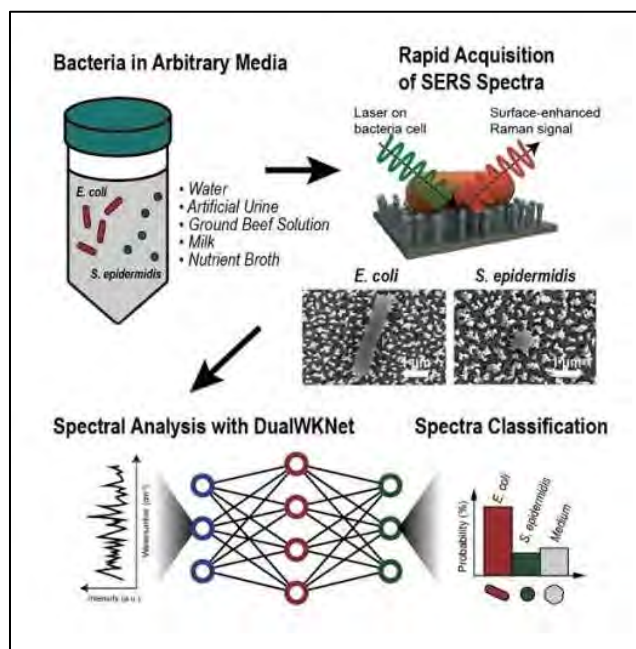


Figure 1 KAIST Process To Rapidly Identify And Classify Bacteria. [M](#)

to use Raman spectroscopy coupled with a newly proposed deep learning model to quickly identify bacteria with 98% accuracy (See Figure 1).^M Novices could acquire this technology and pull harmful bacteria directly from the environment.

Additionally, advancements that improve bacteria survivability will also increase the viability of its use. Bacteria can be very fragile when taken out of a controlled environment, which can present challenges to their “deployment and scale-up.”^M However, researchers at the University of Bristol were able to significantly increase the robustness of bacteria to survive in hostile environments that lack the needed nutrients to keep the bacteria alive.^M Published in the ACS Synthetic Biology journals in February 2022, researchers were able to engineer bacteria to carry a “limited secondary source” of nutrients within itself to activate when resources become sparse.^H

Along with purposeful improvements, bacteria have a natural tendency to develop antibiotic resistance due to “the proliferation and misuse of antibiotics.”^H Published in March 2022, researchers have figured out a way to use X-ray and electron crystallography to map drug-resistant bacteria’s protective layer, which could pave the way for more effective drug development.^M However, the Biotechnology Innovation Organization (BIO) recently stated “the breadth and novelty of the antibacterial clinical-stage pipeline is insufficient to meet the ongoing threat of wide-spread infection from drug-resistant strains.”^M This essentially means that the risk from bacteria is too large to completely tackle and it will remain a threat to human health well into the future.

Bacteria is also specifically attractive for use in biological attacks due to its ease in employment. As with the anthrax example, nefarious actors can simply release bacteria in the air for inhalation or apply it to food as seen in 1984 when a group intentionally released salmonella on a salad bar in Oregon infecting over 750 people with food poisoning.^H Given this, some analysts believe that it is just a matter of time before a bioterrorist uses a sizeable bacterial attack to inflict “widespread damage.”^H Accidental infection also illustrates the ease of employment. As seen in October 2021 when Walmart recalled a scented room spray that contained a rare bacteria leading to two deaths.^M The agents used in these attacks don’t necessarily need to be deadly either. Widespread food poisoning can significantly reduce military combat power for a duration during a decisive point in war.

Due to improvements in pulling and quickly cataloging bacteria from the environment, current and future advancements in bacterium survivability, and ease in employment make it likely (56-70%) that bacteria will remain the pathogen of choice for a biological attack by either a bioterrorist or adversary military through 2035.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time and the task was not particularly complex. Due to the importance of bacteria in the environment, research material is abundant, and the reliability of sources was above average. The sources available did corroborate each other and analyst collaboration was modest.

Author: Timothy A. Harloff

Genetic Synthesizer Advances Highly Likely To Proliferate DNA Editing Technology To The Masses By 2035

Executive Summary

Advances in genetic synthesizers is highly likely (71-85%) to increase the capability and lower costs necessary to conduct advanced DNA splicing by 2035. Despite current high expertise requirements to perform DNA splicing and synthesis, such as a PhD in microbiology, advanced gene synthesizers are lowering this barrier and increasing the number of organizations and people splicing DNA. Further, proliferation of this technology is likely (56-70%) to increase the accidental or intentional release of viral diseases across the world possibly leading to various pandemics.

Discussion

Jennifer Doudna's, PhD, discovery of the CRISPR-CAS9 process of DNA editing in 2012 sparked resurgent interest among research labs and biotechnology companies to use this technology to edit and build gene sequences.^{[M.L](#)} Biotechnology companies such as Caribou Biosciences and Mammoth Biosciences have sought to leverage this technology to develop novel therapeutics for diseases and health conditions.^{[H.H](#)} Increased demand for devices to conduct gene editing has been met by numerous companies seeking to make this process more efficient and cost effective.^{[M](#)}



Figure 1 YouTube Video on How a DNA Sequencing Machine Works.^{[M](#)}

While Frederick Sanger developed the first gene sequencing technique in 1971, rapid advances in gene sequencing did not occur until after the advent of the Human Genome project in 1990.^{[H.H](#)} Effective and efficient gene sequencing requires significant computer processing power that was not available until 2007.^{[M](#)} Advances in computer technology has allowed the scientific community to sequence nearly any biological material to include SARS-CoV-2 in days instead of decades.^{[H.H](#)} These DNA sequences are available throughout the world on open-source databases that facilitate further scientific research and rapid disease response.^{[H.H](#)}

Gene synthesis is decades old with the first automated machine DNA synthesis occurring in the late 1970's.^M Applied Biosciences marketed a simpler machine that performed oligonucleotide synthesis, Model 394, in 1989 that allowed someone with less training to combine short segments of DNA to make a wholly different organism.^M While CRISPR has revolutionized gene editing, gene synthesis using 'olios' (short segments of DNA) is in a revolution as well where scale of production has increased over 1000 fold and costs have decreased by a factor of 10.^M

Rapid advances in computing technology and automation significantly reduced the cost of DNA sequencing and subsequent synthesis.^H As a result, outfitting a lab to conduct genetic sequencing, modification and synthesis would cost tens of thousands of dollars; however, modernization in this field is lowering the cost of these devices to the range of \$2000-\$5000.^M Further, specialized expertise is no longer required to operate these devices as they often have push-button simplicity. It is entirely possible for a hobbyist biologist to outfit a garage lab capable to conducting genetic research and modification.^{M,M}



Figure 2 YouTube Video on Writing the Future with Synthetic DNA.^M

Proliferation of this technology is highly likely to increase the risk of a pandemic outbreak either by accident or intentional release of a pathogen. In 2017, molecular virologist Professor David Evans, PhD., of the University of Alberta was able to recreate small pox cousin from commercially available horse pox in order to prove that advances in synthetic biology could pose a threat to the human race.^H While this feat cost approximately \$100,000, took six months and required status as a researcher to purchase the component parts of the virus, these are not insurmountable barriers to a motivated malign actor, especially if they have any microbiology degree or state sponsorship.^M

Analytic Confidence

The analytic confidence for this assessment is *moderate*. Sources are reliable and derived primarily from U.S. government, reputable research institutions, and scientific journals. The time horizon for this estimate is long and sensitive to change. The analyst worked alone, did not use a structured methodology, and is not an expert in biotechnology nor microbiology; as such greater research into this topic is recommended.

Author: Daniel D. Mitchell

Gene Drive Technology Likely To Increase Risk Of Genetic Based Threats By 2035

Executive Summary

Gene drive technology is likely (56-70%) to increase intentional or unintentional threats to ecosystems when forcing genetic selection of specified traits throughout future generations. Despite the well-intentioned efforts to use gene drive to perform ecological engineering, scientists lack sufficient knowledge of the full scope of genomes to understand how modifications of specific parts will impact the whole. Gene drive also offers malign governments a tool to surreptitiously alter the genomes of human groups that introduce genetic diseases, lethal sensitivities or sterilization leading to genocide.

Discussion

Gene drive is a process where scientists preference the selection of a genetic trait of one parent over another, replacing the natural selection process.^H When this happens naturally, these genetic traits are considered dominant as they drive themselves throughout a population. RNA-guided gene drives offer scientists the ability to select which traits will be dominant (Figure 1).

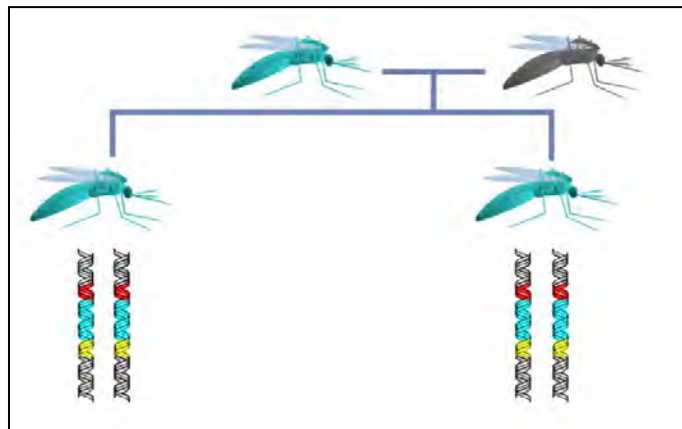


Figure 1 Gene drives may spread genomic alterations through over many generations.^H

Discovery of CRISPR-CAS9 in 2012 as a DNA editing tool has allowed gene drive technology to become more than theoretical.^H CRISPR-CAS9 enables precise editing of short sequences of DNA and replace it with a guide RNA sequence that directs the natural healing process of the body through homologous reconstitution.^H The CAS-9 nuclease can be modified to include a gene drive that make the guide RNA dominant for sexually reproducing organisms as well as genetic transmissibility to offspring.^H

Scientists have already used gene drive technology to modify a mosquito population to reduce its ability to pass along pathogens such as malaria, dengue, yellow fever, and zika.^{H,M} Biotech firm Oxitec released the first batch of these genetically modified mosquitos in the Florida Keys in 2021, reporting that while they saw positive results, they were localized and lasted approximately three generations.^H This was not unexpected as researchers have discovered that unless the gene drive was linked to a genetic sequence required for survival, such as the reproductive gene *doublesex*, that natural gene

mutations would occur to prevent CRISPR from recognizing the specific gene sequence it was designed to target.^H

However, the Oxitec mosquitos serve as an example of the ethical challenges related to gene drive. Many Florida residents were opposed to the Oxitec pilot program fearing the impact to the ecosystem or to humans whom the mosquitos may bite.^H Scientists also warn that robust safeguards and public oversight must be in place to prevent the unintentional negative alteration of an ecosystem.^{H,M} Researchers postulate that additional RNA-guided gene drives could be used to either reverse the initial genome alterations in affected organisms, or serve as a immunizing drive to alter the target of the first gene drive that changes the target DNA sequence thus preventing genetic transmissibility.^H More research needs to be done to validate these theories are effective in the wild. Another ethical concern is unintended consequences as scientists are still discovering which traits are related to specific DNA sequences and how modifications using microRNA strands can cause multiple effects, such as the relation between HIV and Multiple Sclerosis.^H

“Population suppression may be one of the most powerful applications of gene drives.”^H Gene drives can confer sensitivity to a specific chemical, environmental particle, or prodrug that could be activated later within a confined geography or population.^H These sensitizing drives would allow a malign actor to surreptitiously induce mortal risk into a population through injections that could be activated with covert precision that disguise a lethal attack. One possible scenario could include Chinese governmental medical assistance visits to Tibet and Xinjian where they may compel the Tibetans and Uyghurs to receive a false vaccination that contains a sensitizing drive.^M This induced sensitivity may be activated by something normally as harmless as pollen, a medication, or food treated with a pesticide that is approved for human consumption. Gene drive could also be used to induce other human genetic trait selection that could lead to extinction such as producing only male offspring. Gene drive prototypes are less than ten years old and will likely (56-70%) see rapid development through 2035 and beyond.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone, possesses no specialized knowledge in biosciences and did not use a structured method. Given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Daniel D. Mitchell

DNA Computing And Genetic Circuits Likely To Have Military Use By 2035

Executive Summary

Due to continued advances in synthetic biology, it is likely (56-70%) that DNA computing and genetic circuits will be advanced and cost effective enough to have military utility by 2035. Even though both technologies have experienced anemic growth before the 2010s, rapid advancements in AI, machine-to-machine learning, and understanding of genomics mean that DNA computing and genetic circuitry high likely (71-85%) poised to leap forward in practical use. DNA computing has the capability to advance storage and computing beyond silicon and the potential to free militaries from the need for rare earth elements. Genetic circuits have the potential to replace large, bulky digital equipment, particularly in the area of sensor technology.

Discussion

In 1994 researchers at the University of Southern California created the first DNA computer.^{[H.H](#)} Since that time research and development has continued to increase the

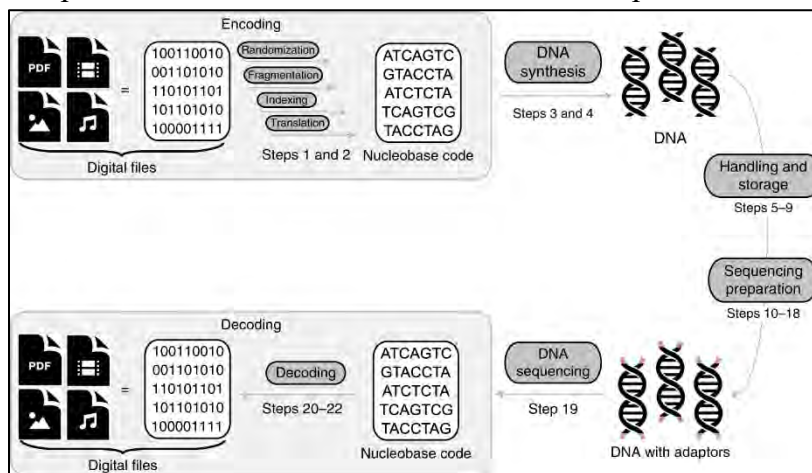


Figure 1 Process of Encoding and Decoding Data into and from a DNA Data Storage Site.^{[H](#)}

capacity of DNA computing and storage technologies. DNA can be used for massive data storage on DNA strands in a very small physical footprint. One estimate is that the data stored in the entire World Wide Web could be stored in a coffee cup of DNA material (see Figure 1).

Genetic circuits are genetically engineered cells which function in the same manner as a computer logic circuit. The cells have a set of receptors that act as sensors. When the cell receptors detect a particular substance, a chemical reaction releases a protein to another receptor. Once this protein is joined to the second receptor, then next chemical reaction triggers a next chemical reaction to create an effect such as triggering phosphorescence or releasing chemicals or medicines.^{[H.M](#)} Figure 2 demonstrates numerous processes that a gene circuit can trigger in a cell.

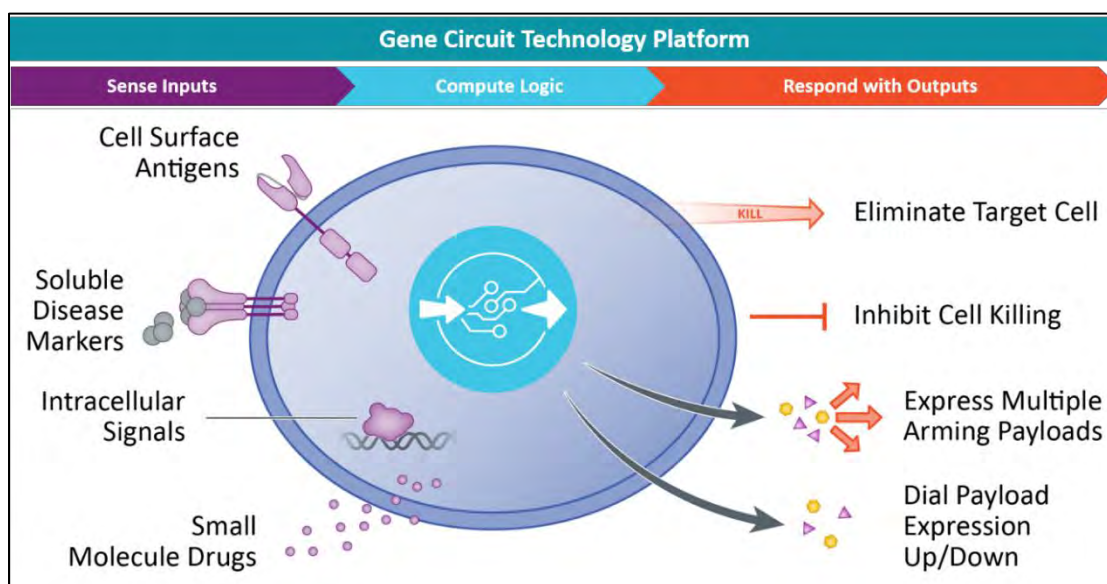


Figure 2 Input-Process-Output Diagram of a Notional Genetic Circuit.^M

Despite the fact that DNA computing and genetic circuit research has taken almost two decades to mature, increasing technological growth in computing power and artificial intelligence has massively expanded the knowledge of and the ability to manipulate DNA and cells to enable researchers to move biocomputing towards practical application.^{M,H} Techniques such as DNA nanoengineering, DNA origami, and enzymatic nicking have made DNA computing and genetic manipulation smaller and more efficient.^{H,H,H} Additionally, industry, academia, and government have taken steps to set conditions for DNA storage common standards. In October 2020, 4 biotechnology firms formed the DNA Storage Alliance (DDAS).^H Since that time over 29 academic, industry, and government organizations have joined DDAS to create "...specifications and standards...to promote the emergence of interoperable DNA data storage based solutions that complement existing storage hierarchies."^H As of January 2022, private firms continue to join the alliance.^M

DNA computing and genetic circuits have some clear potential practical applications for military uses. With the lack of requirement for rare earth elements and special materials, DNA computing offers a cheaper, sustainable basis for storing data.^{M,M} The smaller size of DNA storage could potentially remove the requirement for large bulky communication systems. Current genetic circuit research and development is moving towards their use in medical therapeutics and personalized medicine.^{M,H,M} Those medical uses could be applied to military personnel to assist in keeping soldiers in the fight for longer.^M Additionally, the detection capability of genetic circuitry could be applied for detection of hazardous materials, chemical, biological, radiological, and nuclear material, and embedded in individual soldiers and component materials.^{H,H,M,H}

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple academic and business sources corroborated the growth and potential of DNA computing and genetic circuit, but it remains unclear if the business model or technology will confer enough profit to fund greater expansion. There was adequate time to complete the estimate, however the analyst worked alone and his relative lack of expertise may have left gaps in the analysis. The lengthy time frame of the estimate means the report is very sensitive to changes due to incentive structures which drive industry investment towards practical application.

Author: Matthew S. Rasmussen

Nanobiosensors Protecting Food Security Likely Within Ten Years

Executive Summary

Bio-engineered threats to the national food supply chain make it likely (56-70%) that nanobiosensor technology from Roswell Biotech, NT Sensors, and others will bring to market capabilities to rapidly detect natural and bio-engineered threats to the food chain in the next decade. Despite current biosensor technology and monitoring systems like ProMED, innovative companies are likely to improve and protect food production and security. Nanobiosensors will go from reactive and expensive detection techniques to rapid, cheap, and accurate methods to quickly determine and decipher threats to the national food security system. The ProMED monitoring program does not use advanced sensors and may miss current and future threats. US leaders will require real-time pathogen information to mitigate threats to food, people, and other national security interests.

Discussion

Nanobiosensors research in agricultural biotech has reached a tipping point; even Congress is studying how climate change threatens agroecosystems and food security. [H.H.M.H](#) According to the National Intelligence Council's Global Trends 2040 report, "Biotechnology is likely to make significant contributions to economic growth during the next two decades, potentially affecting 20 percent of global economic activity by 2040, notably in agriculture and manufacturing."[H](#)

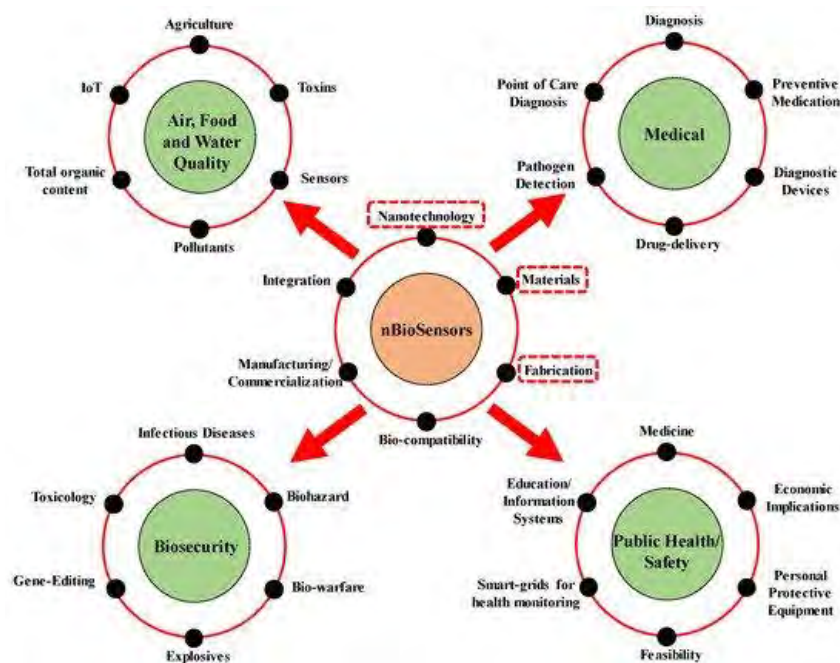


Figure 1 The Primary Applications of Nano-Biosensors can be Broadly Divided into the Following Fields: Monitoring of Air, Food, and Water Quality, Medical Research, Biosecurity, and Public Health and Safety.[H](#)

during the next two decades, potentially affecting 20 percent of global economic activity by 2040, notably in agriculture and manufacturing."[H](#)

Although the Program for Monitoring Emerging Diseases (ProMED) started in 1994, more work is needed to improve reporting and monitoring of threats to food safety from microbial threats (See Figure 1).^{H,H} An estimated \$55B/year worldwide is lost due to plant viruses in agriculture, leading to a need for biosensors that rapidly detect viruses on-site.^H Despite the infancy of nanobiosensors, the advantages of pursuing this technology for food safety are that they are ultra-sensitive and can detect single virus particles at ultra-low concentrations, work at the atomic scale with the highest efficiency, and increase the surface-to-volume ratio.^M Deployable nanobiosensors both inside and outside of plants will better detect threats to food security. Utilizing molecular electronics through “sensitive, rapid, and easy-to-use portable devices for the early detection of viruses in infected plants by in-field or on-site application” will help US industry and the military to sense and respond to threats quickly.^H

Nanobiosensors based on semiconductor field-effect devices (BioFEDs) and complementary metal-oxide-semiconductor (CMOS) technology will advance food security by utilizing detectors capable of single-molecule interactions in real-time.^{H,H} Peer-reviewed technology from Roswell Biotech on molecular electronics chips validate the ability to accurately and instantaneously detect thousands of target pathogens in real-time with future capabilities of 10M biosensors on a single 65nm chip.^H Roswell's technology is currently deployable to detect threats in multiple environments, which will help protect the US military and industry.^M As ProMED is a slower notification system, Roswell's technology incorporated into a national alert system will lead to fast notification of problems in the food supply and other industries.

Technological advances using silicon nanowire field-effect transistors (SiNW-FETs) and graphene field-effect transistors (G-FETs) will improve the accuracy in detecting harmful pathogens.^H MIT researchers are using single-walled carbon nanotube (SWNT)-based near-infrared (NIR) fluorescent nanosensors to detect arsenic down to 6ppb accurately, a world first.^M Using electric nose and tongue nanobiosensors will enable food security throughout the food production and consumption process.^H Going beyond the current technology of monitoring the agroecosystem with basic environmental data nanobiosensors will enable improvements in food production.^M

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were very reliable and tended to corroborate one another. Most sources are from peer-reviewed academic sources. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, this report is sensitive to change due to new nanobiosensors technological breakthroughs with the rapid technological change.

Author: Justin L. De Armond

Cell Free Technology Highly Likely To Be A Bioweapon By 2032

Executive Summary

Cell free technology highly likely (71-85%) to be utilized for nefarious purposes within the next 10 years due to low cost, complexity, and lack of infrastructure requirements. While the technology is possible today, primarily used in therapeutic proteins and diagnostic sensor platforms, subject matter experts in biodefense and biosecurity industries identify cell free technology as a primary area of concern.

Discussion

“Cell-free protein synthesis (CFPS) is a simple, rapid, and sensitive tool required for the synthesis of the desired proteins.”^M The U.S. Army is currently utilizing this in the form of testing capability using BioFire® by preventive medical detachments in operational settings.^H The second most common application of this technology is developing therapeutic proteins to treat cancer, diabetes, and vaccine and virus like particle production (see Figure 1).^M

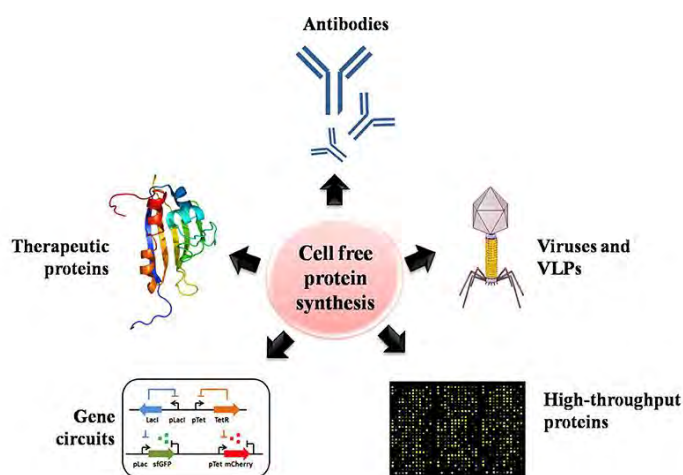


Figure 1 Exploring the Potential of Cell Free Protein Synthesis for Extending Abilities of Biological Systems.^H

The disadvantage of using living cells is the requirement to keep them alive and the necessary infrastructure to do so. To be conducted primarily

on-site, the cells require culture medium and costly tanks. The cells also continue to create a biological process and the process desired to be generated, with additional steps required to purify the specimens for ultimate use. CFPS allows the use of the structures required for transcription and translation within the cell, without the need for the other cellular biomechanics. This can lead to higher protein titers due to the unilateral focus of the process.^M

The development of CFPS is facilitated utilizing low cost and commercially available items. The basic process consists of growing live cells in a liquid culture accomplished via widely available media. Platforms commonly used consist of Escherichia Coli and wheat germ.^M These lower cost, lower complexity mediums provide scalability,

increasing the variability of use, decreasing opportunity costs, and is especially advantageous for difficult to synthesize proteins.^M There are companies marketing the technology and supplies to schools for implementation in science programs.^M

Freeze Dried Cell Free systems are more biosafe and stable than other biological systems, making them highly transportable and minimizing risk to the individual transporting it.^M Another key component making this technology attractive is eliminating the need for cold-chain logistical requirements and can be shelf stable for up to a year.^M The goal is to take this technology to places where large facilities cannot be established.^M It is theoretically possible nefarious actors could place a small ampule of freeze dried protein in an overnight bag, travel via any form of conveyance, reconstitute it with a toxic substance, and unleash it undetected.

Utilizing a Google search comparison of the terms “Cell Free Protein Synthesis” versus “Cell Free Protein Synthesis Bioweapon” yielded a difference of nearly 1.7 billion hits supporting the former. Further scrutiny of the top three pages of CFPS Bioweapon results elicited mis-hits within the search, with less than 30% of the results relating to a valid combination of the search parameters. Indicating while there is some academic and industry interest in how malicious actors can use this technology, it does not appear to be a wide spread area of research or concern.^M

Many properties make bioweapons attractive: low cost, ease of access and manufacturability, stability, low quantity requirements, risk reduction for the deployer, and ability to cause panic.^M Subject matter experts in both the military and academic environments specializing in biodefense have cited this as one of their top emerging concerns.^{H,H} Utilization of CFPS satisfies many if not all these elements.

Analytic Confidence

The analytic confidence for this estimate is *high*. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Enzymes Capable Of Rapidly Degrading Common Plastics Highly Likely By 2035

Executive Summary

Despite plastics' natural resistance to biodegradation and currently available means to degrade them, it is highly likely (71-85%) that industrial biotechnology will produce widely available enzymes capable of rapidly degrading common plastics by 2035. A study published in late 2021 discovered over 30,000 nonredundant enzymes in the environment capable of degrading 10 types of plastics and in 2020 the French company Carbios produced an enzyme from a bug capable of breaking down a plastic bottle in a matter of hours.

Discussion

Humans produce over 380 million tons of plastics globally each year.^M Of the estimated 8.3 billion tons of plastic produced since 1950, people have only recycled roughly 9% of it.^M Most plastic waste ends up in landfills, oceans, seas, and soil subject to natural biodegradation processes that can take as long as 16 to 48 years for a polyethylene terephthalate (PET) bottle under ambient conditions.^H PET, or polyester, is a petroleum-based synthetic plastic most commonly produced globally with numerous applications in the textile, bottling, and packaging industries.^M Additionally, in 2018 the U.S. Army Research Laboratory in cooperation with the U.S. Marines began studying the use of PET in the 3D printing of repair parts to enhance readiness and reduce dependency on logistical supply lines.^M

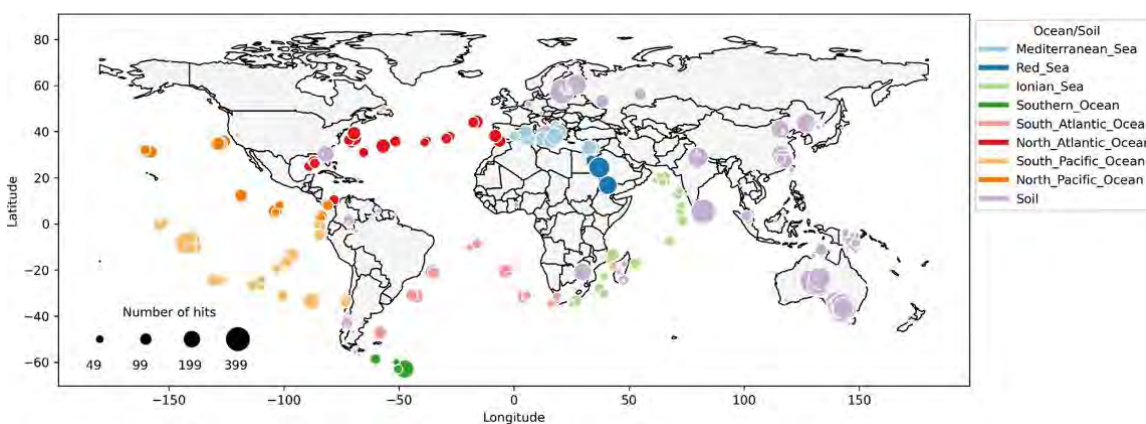


Figure 1 Plastic Degrading Enzyme Discoveries Across the Globe.^H

A study published in the *American Society for Microbiology Journal* in late 2021 concluded that nature is responding to the high levels of plastic pollution in the environment by developing microorganisms capable of degrading plastics.^H Interestingly, the quantity and type of microorganisms discovered correlates to the types and amounts of pollution in the environment.^H According to the findings, researchers identified over

30,000 non-redundant enzymes (11,906 in the ocean, 18,119 in the soil) possessing plastic degradation properties for 10 common plastics (6 polymers and 4 additives commonly used in plastic production) to include PET (See Figure 1).^{[H](#)} This study unlocks enormous potential for industrial biotechnologists to develop novel solutions to the global plastic pollution problem.^{[H](#)} Additionally, given the sheer amount of identified enzymes across the globe, researchers can better study the potentially synergistic effects of microbial communities to degrade complex, composite plastics.^{[H](#)}

This is not the first discovery of its kind nor the only example of the synergistic potential of plastic eating enzymes. In 2016, scientists discovered a colony of organisms using PET plastic as a food source in Japanese waste sites capable of almost completely degrading plastic within six weeks.^{[M](#)} In 2018, researchers produced an engineered version of the same enzyme that started breaking down plastic in a matter of days, which was 20% faster than the naturally occurring plastic-eating bug.^{[M](#)} In 2020, scientists demonstrated the synergistic potential by linking two enzymes found in the colony to create a super-enzyme that started breaking down plastics six times faster than the single enzyme.^{[H](#)} As stated by Professor John McGeehan from the University of Portsmouth, UK, “this is a trajectory towards trying to make faster enzymes that are more industrially relevant,” indicating that commercial application could happen within a year or two.^{[M](#)}

Similarly, a French company, Carbios, published research in the journal *Nature* in April of 2020 regarding their successful engineering of an enzyme capable of achieving over 90% depolymerization of PET in just over 10 hours at 72 degrees Celsius.^{[H](#)} A major advantage of this process is that unlike traditional thermomechanical recycling that reduces the mechanical properties of the plastic, biologically recycled PET offers the same properties as virgin plastic.^{[H](#)} Already partnering with major companies to include Pepsi and L’Oréal, Carbios is seeking to reach industrial scale recycling within 5 years.^{[M](#)} Part of Carbios’ plan is to team up with Denmark based biotechnology company, Novozymes, to mass produce the enzyme while being the first company to bring this technology to market.^{[M](#)} Additionally, Carbios researchers estimate that the enzymes will cost roughly 4% of the total cost of virgin plastic.^{[H](#)} However, given that Carbios will need to grind down and heat the plastic prior to enzyme application, the initial overall cost will be higher than virgin plastic.^{[M](#)} Carbios is not deterred by this fact given the current high prices and high demand for lower quality recycled plastics.^{[M](#)}

Although much of the commercial research and discovery into bioremediation of plastics centers around PET, the future is wide open for more complex, composite plastic degradation. The sheer number of enzymes already in nature coupled with continuing evolution and synergistic potential, make it highly likely (71-85%) that enzymes capable of rapidly degrading common plastics will be widely accessible by 2035.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time and the task was not particularly complex. The reliability of sources available on the bioremediation of plastics was above average with scientific studies and real-world applications available for the estimate. The sources available did corroborate each other and analyst collaboration was modest.

Author: Timothy A. Harloff

Advanced Bioreactors Likely Available To The General Consumer By 2035

Executive Summary

Despite the current high cost of assembling and difficulty in operating fixed bioreactor systems, it is likely (56-70%) that advanced bioreactors capable of growing organisms and creating biological finished goods will become more accessible to the general consumer by 2035. Given the importance of bioreactors in several industries and the natural convergence of technologies, fixed bioreactors will continue to become more efficient, easier to operate, and less expensive. More accessible and advanced bioreactors will allow nefarious actors to produce hazardous biological material more efficiently and at scale.

Discussion

Bioreactors are “the backbone of the bioprocessing industry.”^H

Biotechnologists utilize them to induce biochemical processes from biological materials.^M These processes allow them to grow organisms or create finished products such as biofuels and vaccines.^M A typical bioreactor is a vessel containing the basic components to allow for aeration, agitation, regulation of parameters such as temperature and pH control, as well as a drain to extract both waste and finished product (See Figure 1).^M As an example, Dr. Chaim

Weizmann used a bioreactor to convert poly-sugars from corn and potatoes into the acetone needed to manufacture smokeless gunpowder during WWI.^M Today, biotechnologists use bioreactors to create many products within the food, pharmaceutical, and cosmetic industry.^M

Tissue engineering is another significant area of research that utilizes bioreactors. In this field of study, scientists add scaffold systems and biosensors to traditional bioreactors.^H Scaffolds allow cells to form into 3D structures and biosensors monitor cellular activity.^H This combination allows scientists to better study cellular processes and interactions in the pursuit of more effective therapeutics, develop skin grafts, and to potentially grow full organs suitable for transplant in the future.^{H,M}

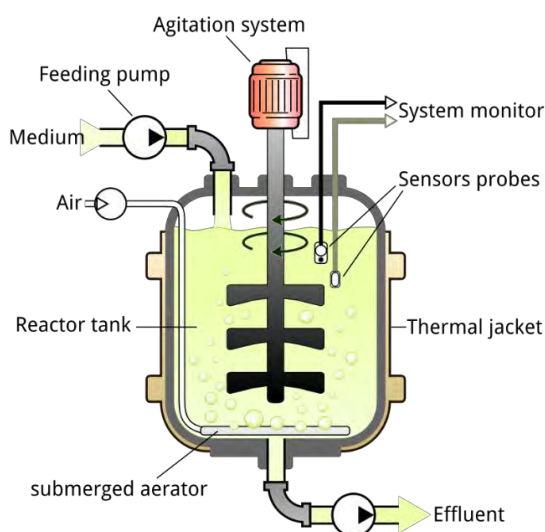


Figure 1 A Diagram of a Simple Bioreactor Design.^M

Based on the importance and many applications of bioreactors, scientists are looking at ways to redesign the current hierarchal control system into a flat organizational control system (FOCS) by integrating smart sensors, actuators, artificial intelligence, and cloud computation.^H These upgrades will improve overall process control while increasing efficiency, robustness, and lowering costs.^H

Despite the advantages of bioreactors, maintaining a fixed bioreactor system is currently expensive. This high cost leads many manufactures, particularly in the pharmaceutical industry to employ single-use bioreactors.^H However, single-use systems have limitations when trying to produce large quantities of biological material.^H As stated by Dr. Vijay Singh, “disposable bioreactors have demonstrated how inefficient, costly, and difficult to operate” traditional bioreactors are, suggesting that this phenomenon will continue to spur better designed systems in the future.^M Additionally, as sustainability concerns continue to rise and costs drop, manufacturers will likely favor advanced fixed bioreactors capable of mass production.

Based on the convergence of traditional bioreactors with AI, smart sensors, and advanced computing coupled with the continuing drive for development, it is likely (56-70%) that advanced bioreactors will become more accessible, cost effective, and attractive for the general population. During the COVID-19 pandemic, DIY enthusiasts attempted to produce a vaccine quicker than industry.^M More accessible bioreactors would allow DIYers to produce unregulated “vaccines” rapidly and in bulk.

More accessible and advanced bioreactors could allow nefarious actors to manufacture harmful organic material or material that they can use in a harmful manner more efficiently and at scale. As an example, while the war in Ukraine brings attention to the global energy market, ecoterrorists could manufacture numerous known bacteria capable of damaging oil reserves.^M Gaining access to a virus, bad actors could also use bioreactors to discreetly grow more virus as demonstrated by scientists experimenting with the influenza A virus in 2019.^H As advanced bioreactor technology proliferates, costs will reduce to the point that motivated individuals will gain access and benefit from the ease of use that will be inherent in future systems.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time, but the task was complex based on the technical nature of the topic. The reliability of sources available on bioreactors was above average with scientific studies available for the estimate. The sources available did corroborate each other and analyst collaboration was modest.

Author: Timothy A. Harloff

Deep Mind's AlphaFold Likely To Have Weaponizable Dual Use For Proteins, Enzymes And Toxins

Executive Summary

AlphaFold's ability to predict protein structures with near experimental results is almost certain (86-99%) to dramatically impact biotechnology research and development in a greater understanding of the relationship between protein structure and function, drug development, and enzyme modification. Google's affiliate Deep Mind has created a paradigm shift by solving one of the most difficult problems in biology.^{[H](#)} Despite the enthusiasm among researchers over AlphaFold, it is too soon to determine how deep learning AI will disrupt the biotech field; however, it is likely (56-70%) that these developments will be of dual use research of concern (DURC) by 2035.

Discussion

AlphaFold is Deep Mind's software that can predict the shape of protein structures from its composite amino acids to approximately a 90% accuracy.^{[H](#)} Deep Mind first demonstrated the effectiveness of AlphaFold during the 2018 Critical Assessment of Structure Prediction (CASP), a competition that specifically aims to enhance the area of predictive protein folding.^{[H](#)} AlphaFold greatly outperformed the competition in 2018 and then again in 2020, producing results that were almost at the same quality as determining shape from experimentation.^{[H](#)}

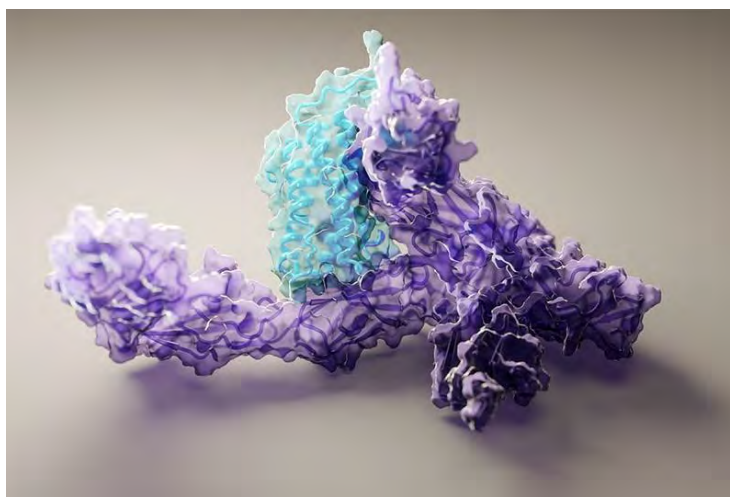


Figure 1 YouTube Video Explaining Deep Mind's AlphaFold.^{[H](#)}

Accurately determining protein structures has long been an important problem for researchers to solve. Proteins gain function when they fold into shapes from their long linear amino acid chains.^{[H](#)} These structures determine how these proteins function, how they interact with other proteins, ligands, and how their processes can be affected with an outside material like a drug.^{[H](#)} Proteins control biological processes in living beings and understanding structure directly correlates to understanding functionality.^{[M](#)}

Scientists have been working on determining protein structures since the 1950s.^{[H](#)}

photographed using x-ray crystallography, or more recently cryo-EM; then shapes are analyzed and measured if the image and structure allow it.^H Researchers often spend ten years or more trying to determine the exact shape of a protein.^{H,H} AlphaFold can do it in minutes to hours with only the component amino acid information.^H AlphaFold's prediction provides a starting point that researchers can validate in dramatically less time than by original experimental determination.^H

While a paradigm shift, AlphaFold has its limitations. The deep learning AI software was trained with hundreds of thousands of known protein structures.^H As such it is not yet able to accurately predict several non-evolutionary single sequences such as mutations, drug interactions or proteins that can take on multiple structures naturally.^H Proteins can exhibit dynamic behavior and flexibility that AlphaFold is unable to predict at this time.^H However, Deep Mind improved AlphaFold after CASP 2018 to include the ability to predict multi-protein complexes and named it AlphaFold-Multimer.^H

AlphaFold-Multimer demonstrates the rapid evolution of AI technology and the ability to respond quickly to the real-world demands. Deep Mind CEO, Demis Hassabis has said that AlphaFold is the greatest contribution of AI to scientific knowledge and has founded Isomorphic Labs as a focused collaboration with the biosciences community to advance understanding and drug development.^H Hassabis is likely to iterate AlphaFold to have additional functionality to address the problems it currently cannot solve.

AlphaFold has great potential to enhance understanding of biological processes and contribute to drug development, enzyme discovery and general scientific knowledge; however, this understanding is likely to be of dual use research of concern. Greater understanding of protein folding could also lead to understanding of how proteins fold improperly, which often produces allergens, toxins, and prions that can lead to degenerative diseases.^{H,H} Advanced understanding of proteins are also likely to lead to a greater ability to engineer more lethal, weaponized toxins and pathogens. AlphaFold is less than five years old, yet it has disrupted the structural biology field, created spinoff technology, and showed transformative potential; yet, this potential is likely to also lead to greater threats.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone, has no specialized biology training or expertise, and did not use a structured method. This report is sensitive to change due to new information over a long timeframe.

Author: Daniel D. Mitchell

China Almost Certain to Use Genetics as a Part of Surveillance by 2025 That Threatens U.S. Security and Economic Prosperity

Executive Summary

China almost certain (86-99%) to use genetics as part of domestic surveillance by 2025 due to the availability of data and rapid advancements in DNA sequencing. However, there is also strong potential for weaponizing this capability against their foreign adversaries. China has both the capability and intent to use genetics to enhance security, which they can also use to against U.S. government officials, intelligence agents, civilian businesspeople in ways that threaten U.S. national security.

Discussion

Chinese security officials are forcibly collecting the DNA and biometrics of its citizens, especially the Uyghur Muslim minority and the Tibetans both overtly and clandestinely through medical assistance since the early 2000's.^{[H.H](#)} Collection also extends to average Chinese



Figure 1 YouTube Video Illustrating How China is Using DNA to Track Muslim Uighurs in Xinjiang.^{[M](#)}

citizens (Figure 1) having become a part of the regular application process for an identification card, a residency permit, and other government issued licenses and permits. Police are routinely collecting DNA from groups considered a domestic threat: college students, activists, human rights lawyers, migrants, or anyone who happens to be in a hostel, entertainment venue, internet cafe, or rental home.^{[H](#)} Police and military collection of DNA typically accompanies collection of other biometrics like fingerprints, voice prints and facial pictures, along with Personally Identifiable Information (PII).

Despite DNA's critical use in helping the police to solve crimes, Chinese actions and history indicate they will use these for surveillance of their population. DNA sequencing technology is consistently reliable, has push button simplicity, and is about the same cost and size as a cell phone.^{[H](#)} Security officials in Xinjiang have ordered DNA sequencers, PCR amplifiers and genotyping kits.^{[M](#)} Additionally, the Chinese government has amassed the largest DNA database in the world in their National Genebank,^{[H.M](#)} operated by Beijing Genomics International (BGI); BGI is closely connected to the Chinese government^{[H](#)} and routinely collaborates with the People's Liberation Army (PLA) for

genomic research.^M Further, they are testing if the human genome can be used to inform facial recognition through predictive analysis.^M They have all the elements necessary to use genetics to enhance surveillance domestically and are experimenting with implementation now.^H

China is well known for engaging in cyber-attacks to collect vast troves of PII information from U.S. citizens and government officials.^H The most significant Chinese breach of U.S. Government systems was the Office of Personnel Management (OPM) hack of over 21.5 million government employee records stolen, to include the sensitive information found in security clearance background checks.^H Other Chinese cyber hacking has targeted Anthem Health stealing the PII of over 71 million customers.^H Should the Chinese successfully hack the Armed Forces Medical Examiner System, DNA Identification Laboratory (AFMES-AFDIL) Secure Family Reference Database they would be able to correlate the DNA information of Service Members from the past 50 years with stolen OPM data.^H

Because DNA is absolutely reliable for identification, it can be used for blackmail, recruitment for espionage, or public shaming for a past indiscretion by a relative. Finally, should the Chinese begin using DNA identification at their customs offices, it is possible they could reveal the true identities of undercover officials. China's current use of genomic biometrics and focus on creating a security state indicate that they have the intent to leverage their current genetic tools to enhance their security in ways that could harm U.S. security and economic stability.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. The analyst is not an expert on genetics or microbiology. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Daniel D. Mitchell

Weaponized Artificial Intelligence and Blockchain Highly Likely to Threaten Agriculture in Ten Years

Executive Summary

Competitors weaponizing Artificial Intelligence (AI) and blockchain-enabled agriculture are highly likely (71-85%) to impact all aspects of food security in the next decade. Despite AI and blockchain being relatively new in agriculture, the farming industry will make significant investments in AI and blockchain to ensure secure agricultural transactions, more robust plants, remote monitoring of irrigation, diseases, and pests, autonomous planting and harvesting machinery in fields and vertical farms, and predictive analytics. Connectivity to low-powered Internet of Things (IoT) sensors and blockchain agriculture management advances will positively impact the global agricultural business. Competitors will develop their own blockchain and AI agricultural systems that rival the US.^M This requires caution if the US integrates competitor systems that work remotely or via AI autonomous systems incorporating weaponized AI or blockchain that might cause harm to western food production and systems.

Discussion

As AI and blockchain integrate into all aspects of industry, both technologies are likely to create threats and opportunities to food security, which might degrade military sustainment capabilities. Estimated revenues from an AI-enabled agriculture system will be over

\$11B by 2030.^M Agriculture AI systems will change farming and improve food production to both traditional farming and the more modern vertical farming revolution. AI and robotics will assist food production from analyzing satellite imagery, in-field monitoring, assessing crop and soil health, predictive analytics, and autonomous farming machines (see Figure 1).^M

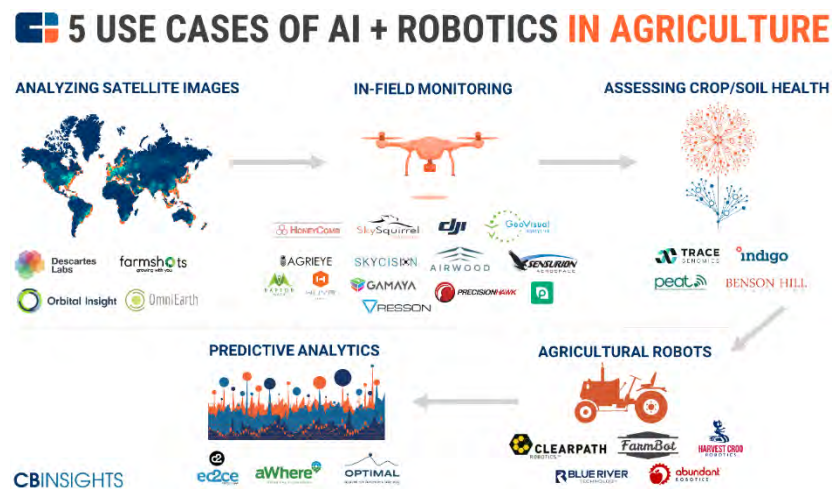


Figure 1 Artificial Intelligence Use Cases in Agriculture.^M

Agricultural supply chain fraud results in a loss of trust and revenue, and utilizing various Industry 5.0 technologies will improve the food chain system.^{H.H.H} Blockchain and IoT integration with the agricultural supply system applies to food consumption, quality, safety monitoring, food safety across the supply chain, food product traceability,

addressing food waste, and inventory management.^H Blockchain technology challenges are the complexity of the supply chain, developing consumer trust, security and awareness of the blockchain technologies, and legal hurdles to implementation across the food supply system.^H Adversaries might hack into IoT systems or damage those systems with targeted physical or cyber attacks, degrading blockchain activities.^H

The use of remote sensing and a mix of stationary and drone-based food production monitoring will provide real-time information to farmers. Satellite imagery provides information on air moisture, water levels, soil conditions, crop yield forecasting, and pest and disease monitoring.^H AI advancements will monitor current conditions and address any issues to food production based on AI recommendations.^H Scientists stated, “AI and machine learning (ML) can assist in identifying those areas most at risk of invasions/outbreaks as well as assisting in plans to mitigate the spread of invasives or diseases.”^H

Precision agriculture utilizing AI models will help farmers obtain the highest yield as machine learning algorithms will help decide “best yield crop by just measuring” multiple parameters.”^H Drones, although currently cost-prohibitive, when connected via the IoT and part of an AI system, improve food production with the implementation of irrigation, weeding, and fertilizer recommendations.^H Competitors are likely to develop similar technology capable of improving their own food production. However, they might also develop methods to degrade our food production by finding vulnerabilities within the security of AI and blockchain systems.

Climate change will require scientists to find new ways to improve plant toughness. A method is AI predictive analytics in agriculture that accelerates the development of more climate-resilient plants.^H Ensuring the needed crop production due to changing climate necessitates incorporating big data, AI, and bioinformatics from “phenomics and genomic datasets” to guide development on smart crops that withstand more variable conditions.^H A danger here is that competitors might sabotage data to protect crop development and harm US research on similar climate-resistant crops. Additionally, a reprogramed AI developed over 40,000 new toxins within six hours.^H Adversaries might weaponize AI to find ways to harm the US military and other industries.

AI challenges associated with agriculture include data acquisition, access, quality, trust, yield prioritization over ecological integrity, and deploying AI/ML at scale.^H Additional AI tasks are governance mechanisms such as data stewardship, ownership, cooperatives, responsible innovation, and risk-informed deployment in off-network digital systems.^H The government and industry must ensure the security of AI applications to deter adversaries from impacting food security and other US industries. Competitors are likely not to follow international norms regarding responsible innovation. The AI and

blockchain systems the US develops to monitor and protect food production should be flexible enough to detect such activity.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources are reliable and tended to corroborate one another, but the original sources used to compile the accessed reports were not always available. There was adequate time, but the analyst is not an expert, worked alone, and did not use a structured method. Furthermore, given the lengthy time frame of the estimate and its reliance on emergent AI, this report is sensitive to change due to new information.

Author: Justin L. De Armond

Cyberbiosecurity Highly Likely To Be A Significant Driver Of Defense And Industry Spending By 2035

Executive Summary

It is highly likely (56-70%) that the protection of biological and biotechnological research and production will consume a significantly greater portion of defense and industrial budgets by 2035 due to the increasing digitization of biotechnology research and the increase in nefarious cyber activity. Wide ranging non-state, state sponsored, and state threats have expanded cyber attacks across the spectrum of industry and government and begun to target biotechnological and bio manufacturing in particular. Stakeholders with interests in biotech research, are highly likely (71-85%) to put increasing pressure on governments, academia, and industry to invest more resources into cyberbiosecurity due to the major threat in the cyber domain to research and development.

Discussion

Increasing digitization and computerization of biotechnological research makes biotech more vulnerable to cyber attack. AI, machine learning, machine-to-machine communication have increasingly permeated biological research and biotechnological innovation. [M,H,H](#) Digitization of mapping of genomes and genetic material are common place. Current forecasts from industry and governments across the world anticipate that it is highly likely (71-85%) that biotech advances will effect medical, agricultural, and social aspects of society. [H,H,M](#) Given the increase in digitization of biotech research and increased penetration of biotech innovation into society, the risk of malign actors exploiting a link or a part of the chain from research to production to supply to consumption. [H](#)

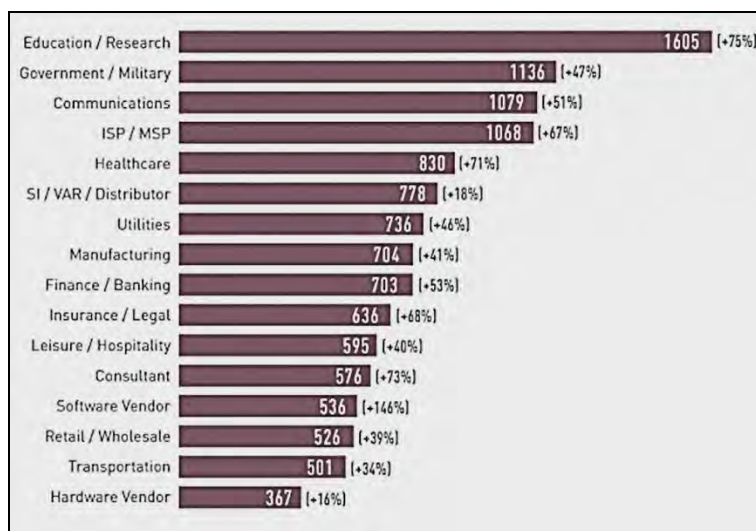


Figure 1 Targets of Cyber Attack by Industry in 2021 with Percent Increase over 2020. [M](#)

The COVID-19 pandemic saw the a significant increase in cyberattacks against biotechnological research and industry. [M](#) With the increase in home telework during the pandemic, cyber attackers began to ramp up the numbers and types of attacks. [M](#) There are multiple reasons for this increase but two of the most prevalent were lack of personal

computer cyber security measures and human error which creates “cyber insecurity.” The massive increase in cyberattacks throughout 2020 and beyond translates to more experienced cyber attackers, making it highly likely (71-85%) that cyber attackers will continue to press their advantages and expand their target set to larger, more complex targets.^{[H.M](#)}

Cyberattackers seek to disrupt both research for nefarious reasons and for profit. The most prevalent attack method currently is ransomware.^{[M](#)} Ransomware is a hacking activity that hacks into data and locks it until the victim pays the attacker. Applied to biological data, hackers could seize DNA mapping, personal DNA data, or biological research for ransom. While non-state actors are responsible for the recent increase in cyber attacks, FBI warnings from Thanksgiving 2021 and the US 2022 Intelligence Community Annual Threat Assessment points to China, Russia, and Iran as top cyber threats to US digital and physical infrastructure.^{[M.M](#)} Thus, academia, industry, and government biotechnology research and production are increasingly at risk from cyberbiosecurity threats.^{[M](#)}

Cyberbio-attackers have also proven their ability to target specific biological data beyond simple ransomware or hacking attempts.^{[H](#)} Researchers at Yale and Ben-Gurion University in Israel have demonstrated how hackers can penetrate synthetic biology databases to place malicious code or toxic DNA sequences into DNA sequences to make synthetically engineered DNA toxic to the recipient.^{[M.H](#)} In spring and October of 2021, biomanufacturing firms in the US were hit by a malware called “Tardigrade” which is a “metamorphic” malware system that acts autonomously to hide inside computer systems

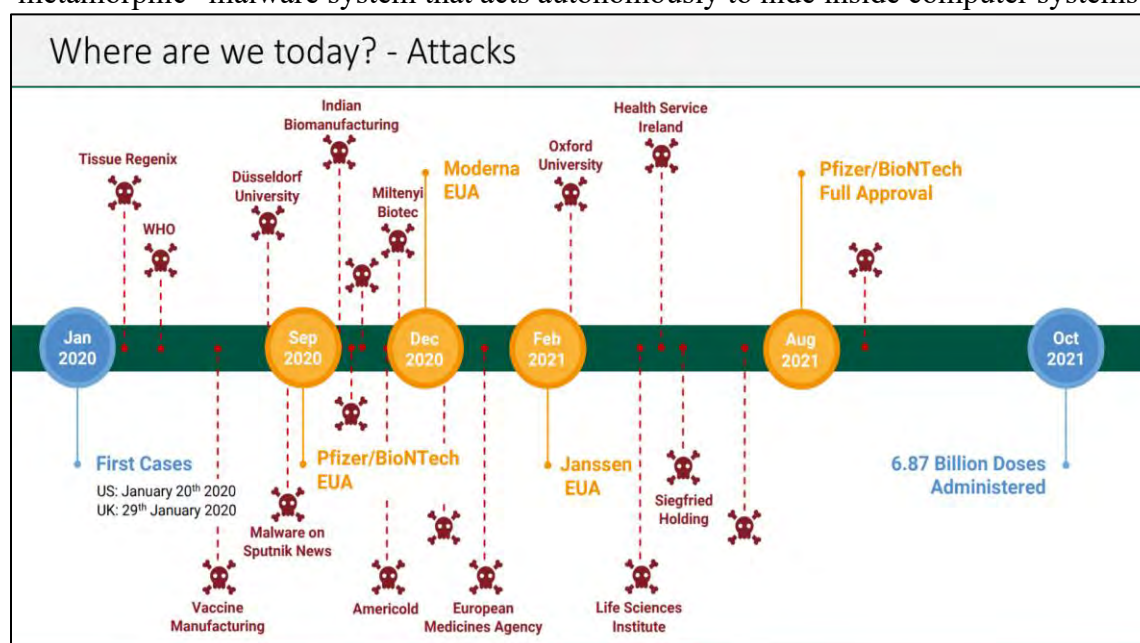


Figure 2 Shows Recent Cyber Attacks on Biotechnological Research and Industry.^{[M](#)}

and funnel data out without need to for external control.^M Given the conditions and experience gained by cyberattackers in the COVID-19 Pandemic, the spread of cyberattacks on biotechnological research and industry, and the specifically targeted cyberbiosecurity threats demonstrated in 2021, it is highly likely(71-85%) that cyberbiosecurity will be a major area of risk in the future.^H Multiple academic and industry sources are advocating for more government regulation on cyberbio laws, regulations, and protections.^{M,H,H,M}

The continuing severity and growing recognition of the cyberbiosecurity threat means that industry, academia, and government, the Army included, are highly likely (71-85%) to be required to place an increasing amount of resources towards cyber protection.

Analytic Confidence

The analytic confidence for this estimate is *high*. Multiple academic, government, and industry sources corroborated the seriousness of the cyberbio threat, increased penetration of digital technology into the field of biotech, and the growing concern of experts throughout the field about cyberbiosecurity. There was adequate time to complete the estimate and while the analyst generally worked alone, peers reviewed the progress and made recommendations. Barring a massive unforeseen change in the use of the computers, AI, and digitization in modern research and industry, the cyber domain will continue to grow in importance, making this analysis less sensitive to change over time.

Author: Matthew S. Rasmussen

Virtual Reality Highly Likely To Increase Access To Biotechnology By 2035

Executive Summary

Despite the high-cost and resource intensity required to learn and experiment with biotechnology, it is highly likely (71-85%) that virtual technologies will increase access to aspiring biotechnology professionals and novices by 2035 who will create new biotechnology capabilities and uses. Virtual Reality (VR) continues to permeate industries across the globe and market projections show a substantial increase from now through 2030. Biotechnology students have demonstrated increased learning with VR and professional biotechnologists have utilized VR in real world applications. The potential exists for nefarious actors to use these same benefits to self-educate and experiment in harmful ways.

Discussion

Virtual Reality (VR) is “the use of computer technology to create a simulated environment” for human interaction using hardware devices such as headsets, controllers, and even treadmills.^M Despite society considering VR to be a “nascent” technology, it is permeating numerous areas within industry to include healthcare, education, manufacturing, logistics, entertainment, tourism, and the military.^{M,M} Additionally, Statista projects a tenfold growth in market size from \$30.7 billion in 2021 to \$270 billion by 2024 with other projections showing a 15% annual growth rate through 2030.^{M,M} Finally, advancements in 5G technology (high-bandwidth, ultra-low latency) and advanced computing will further encourage “the adoption of virtual technology.”^M

Biotechnology, as with other scientific fields, requires rigorous study and the ability to visualize complex structures.^M VR is showing tremendous promise in improving student comprehension and “could offer new entry points to learners.”^M A PhD in biotechnology founded the Danish biotechnology company Labster that is the “world’s leading platform for virtual



Figure 1 Researchers Interact With Molecules in Virtual Reality.^H

labs” claiming to increase student’s grades by over 16% using immersive environments.^{[M,M](#)} Labster designs 3D immersive environments to provide students a unique and memorable learning experience spanning all aspects of biotechnology to include animal genetics and bacterial cell structures.^{[M](#)} Harvard, MIT, and the University of Hong Kong are employing Labster technology to teach their students.^{[M](#)} Another company, Immersive Science, designed a VR tool called ConfocalVR to allow researchers “to visually step inside...cells and see the things they never saw in 2D” when using traditional microscopy.^{[H,H](#)} Data and models derived from this type of technology can be shared across biotechnology communities to expand the knowledge base and allow multiple researchers to contribute their expertise.^{[M](#)}

Traditional biotechnology research is expensive requiring access to various resources and advanced labs to facilitate experimentation, which VR enables biotechnologists to overcome.^{[M](#)} By using simulated labs, researchers can gain access to the most updated biotechnology equipment and methods without the challenge of reserving lab time.^{[M](#)} They can also gain access to a variety of simulated biomaterials without the need to procure, store, and continuously monitor potentially dangerous material which is an advantage in “a field that demands real experiments.”^{[M](#)} As they mature, these simulated environments could also enable researchers to fail early and often through experimentation without wasting bioresources or spending inordinate amounts of capital.

Outside of education, there are real world examples of VR being employed in biotechnology today. In May 2020, researchers used VR to evaluate several COVID-19 protease inhibitor drug candidates by interacting with life size molecules in a simulated environment (See Figure 1).^{[H](#)} Additionally, a biotechnology company Thermo Fisher Scientific invested over \$55 million in VR in 2019 to train 20 workers employed on their drug production line simultaneously.^{[M](#)} In April 2021, Pfizer plans to introduce VR technologies into their sterile injectables plant touting that it will be “one of the most technically advanced” plants in the world.^{[M](#)}

As VR and other technologies that support it continue to mature, it is highly likely (71-85%) that virtual technologies will increase access to biotechnology for aspiring professionals and novices between now and 2035. While this technological convergence offers several benefits to biotechnology, nefarious actors could utilize the technology to self-educate and experiment in harmful ways. Virtual labs present a safe and inexpensive method to access simulated biomaterials and the latest scientific equipment discretely. Additionally, VR could allow nefarious actors to work collaboratively with others in a distributed manner which could hide any malicious intent.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time and the task was not particularly complex. The reliability of sources available on the potential advantages of virtual technologies in biotechnology education and experimentation was above average. The sources available did corroborate each other and analyst collaboration was modest.

Author: Timothy A. Harloff

Additional Findings



BIOTHREAT
FORGE

China's Genomic Research Likely to Exceed U.S. by 2035 Enabled by Massive Collection of Human DNA Samples

Executive Summary

China's massive collection of human DNA samples and formation of government databases make it likely (56-70%) that Chinese genomic research will surpass U.S. research by 2035. Despite current U.S. qualitative advantage in this field, the Chinese government's investment in quantum computing, artificial intelligence (AI), formation of genetic databases^H and strategic biotech acquisitions are likely to erode this advantage. Chances are better (46-55%) that China will gain a qualitative advantage on biological weapons due to unethical research into the genetic modification of humans, animals, and plants.

Discussion

The Chinese government named biotechnology as one of the five strategic industries they were focusing on in their 13th Five Year plan (2016-2020) as they expect it to lead to new horizons for human production and life.^H China's 14th Five year plan (2021-2025) specifically highlights that they intend to use genomic research results to

innovate in the areas of genetic breeding, synthetic biology, in vitro diagnostics, pharmaceuticals, vaccines, and create new crops, livestock, and aquatic products.^H China followed through on their past 5 year plans, aligning their government resources against their priorities; therefore, China is likely to continue accelerate their bio-enterprise development as indicated in their current plans.

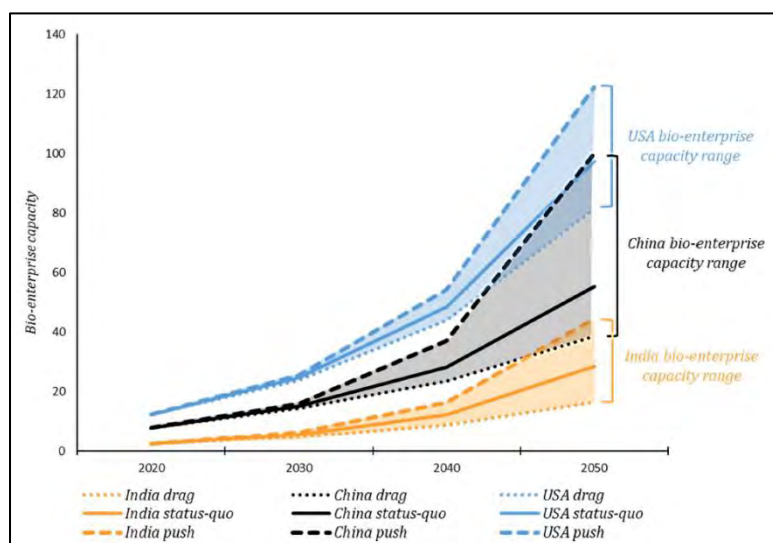


Figure 1 Bio-Enterprise Capacity Scores for Top Three Nations, 2020 through 2050.^M

Despite projections that it will take until 2050 for China to surpass the U.S. (Figure 1),^H China is using strategic acquisitions of U.S. companies to close the U.S. biotechnology gap and gain access to consumer genomic data.^M Beijing Genomics Institute (BGI) acquired Complete Genomics, a U.S. company, in January 2013 to make a leap ahead in gene sequencing equipment, intellectual property rights, and domestic production capability and capacity.^H BGI has sought various partnerships with U.S. hospitals and

research institutions for the same purpose.^H BGI is closely connected to the Chinese Government (PRC)^H with several high level government officials leading the company, and collaborates with the People's Liberation Army (PLA) for genomic research.^M It is the center of the Chinese gene industry as well as owning and operating the Chinese Gene Bank.^M China's WuXi Pharma tech also acquired a U.S. company NextCODE Health in 2015 to form WuXi NextCODE Genomics.^H WuXi has also purchased a Pfizer manufacturing plant in China and a stake in U.S. consumer genetics company 23andMe.^M

China is already collecting massive amounts of human DNA information from both their citizens and from people around the world. China has forcibly collected DNA and biometrics from its Muslim minority Uyghur population ages 12 to 65 yrs.^{M,M} Further, BGI prenatal DNA tests have been a source of over 8 million samples from around the world.^M This information is going into the China National Genebank that has between 100 to 140 million human, plant, and animal DNA samples.^M SARS-COV2 response was also a boon to BGI's efforts to expand their reach into more countries across the world – they set up labs in 18 countries for COVID testing and sold COVID test kits to 180 countries.^M Finally, Chinese hacking groups have targeted healthcare companies to steal Personally Identifiable Information (PII).^H

Chinese focus on quantum computing and AI are likely (56-70%) to accelerate their analysis of the human genome. Quantum computing offers the ability to exponentially increase the speed of problem solving.^H AI advancement provides creative problem solving that can mimic human intelligence.^H Gene databases are basically massive data sets that can be used to find similarities and differences that unlock the purposes of DNA segments. Quantum computing and AI will aid researchers unlock the secrets of gene sequences that can provide a qualitative military or economic advantage in biotech.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another but the researcher is not a biotechnology expert. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Daniel D. Mitchell

Malicious Actors Likely To Utilize Public Health Threats For Global Bioterrorism Within 5-7 Years.

Executive Summary

Readily available resources and low complexity of development make it likely (56-70%) malicious actors will utilize previously known public health threats and emerging biologic pathogens as a source of global bioterrorism within the next 5-7 years. Global attention recently has been placed on novel diseases such as COVID-19, and remains directed towards diseases with high morbidity and mortality. The capability of nefarious actors to develop mechanisms to deliver infectious diseases instilling public fear and instability is increasing. Despite the United States having robust medical infrastructure, the most recent pandemic has indicated pathogens deemed a high priority and the highest risk to national security can be an easily obtained and accessible existential threat for malicious use.

Discussion

The classification of bioweapon diseases as determined by the Centers for Disease Control and others classifies Category A and C as the most significant to public health and national security.^{M,H}

Historically, diseases of public health were given less attention in regards to biodefense, opting for increased focus on more novel or high-risk conditions such as Anthrax and Marburg. A family of viruses, known to cause the common cold to what is now known as COVID-19, has broadened the scope of what is considered a threat to national and individual security.^{H,H}

Pathogens with limited or unknown prevention/treatment options are growing in concern for its threat potential. considered a public health threat.^H Bioweapons and bioterrorism have been a known



Figure 1 Pandemic Preparation Global Health Security Index.^M

threat since at least WWI, and UN (United Nations) Treaties have now prohibited its use. Not all nations adhere to the provisions within the Biological Weapons Convention, nor is it universally signed, and does not account for non-state actors.^{H,M}

Obtaining the necessary equipment and provisions to grow, or modify biological material outside of a commercial lab can be easy and unexpensive. Major Jeff Kugelman Chief of microbiology at USAMRIID indicated he could establish a home lab for around \$2000.^{Annex E} He further stated someone with basic lab experience or a post-doctoral student in microbiology, or a similar field, could easily accomplish. In 2013, a Ph.D. in a Massachusetts apartment for \$500 established a genetics lab.^M Multiple sources indicate creation of bioweapons outside of conventional labs is increasing likely due to ease of procurement of component materials via internet sources.^M How to manufacture personal vaccines^{M,L}, or growing bacteria at home^{L,M,M} takes minimal effort to acquire by open sources via the internet with step-by-step instructions an individual with basic scientific knowledge could accomplish the construction.^M The unlawful potential genetic or biological manufactured material can have is compounded by the inability to trace origins to the manufacturer, making it attractive for malicious use.^M

COVID-19 has shown how ill-prepared countries were for a mass public health issue, or a global pandemic. According to the World Economic Forum, concerns continue for the near future.^H The pandemic exposed how medical threats can identify and exacerbate societal tensions, gaps in infrastructure, governmental distrust, and increase nationalism and xenophobia.^{H,H} The past several years has served as an outline for how adversaries with easily obtainable and manufactured biotechnology can disrupt societies, economies, and political infrastructure, common strategies for malicious use.^H

Analytic Confidence:

The analytic confidence for this estimate is *high*. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Security Standards In India Make High Risk Biosafety Labs Risky

Executive Summary

India's attempt to increase Biosafety Laboratory (BSL) capability for manufacturing and research purposes in response to industry demands, projected growth of the biotechnology sector, coupled with lack of laboratory safeguards, and governmental regulation make it highly likely (71-85%) an accident affecting regional health security will occur. India has made progress in some safety standards since 2019. However, organisms found within BSL 3 – 4 laboratories have high transmissibility rates, and with the geographical locations of high containment labs near densely populated areas and the rapid industry growth in the region make laboratory leaks of such agents opportune.

Discussion

India is one of the top 12 locations for biotechnology manufacturing and research locations globally, with increasing market share (see figure 1).^M In 2017 India made up 3% of the global biotechnology market, and forecasts predict it will exceed over \$100 billion in worth by 2025.^L Some

forecasts project that the bioeconomy will have growth rates totaling 30% by 2025.^M

India is a significant supplier of therapeutic pharmaceutical manufacturing producing over 60% of the global vaccine supply.^M A key element in this process is the utilization of BSL labs of adequate complexity and capacity to support demand. India has six BSL 3 labs, two BSL 4 labs, and an animal research lab characterized as BSL 3+.^{M,M}

While universally accepted safety and policy procedures for BSL 3-4 labs are in place, no overarching authoritative body has governance ensuring compliance.^H The Global Health Index rates India 66th out of 195 countries in safety and preparation for

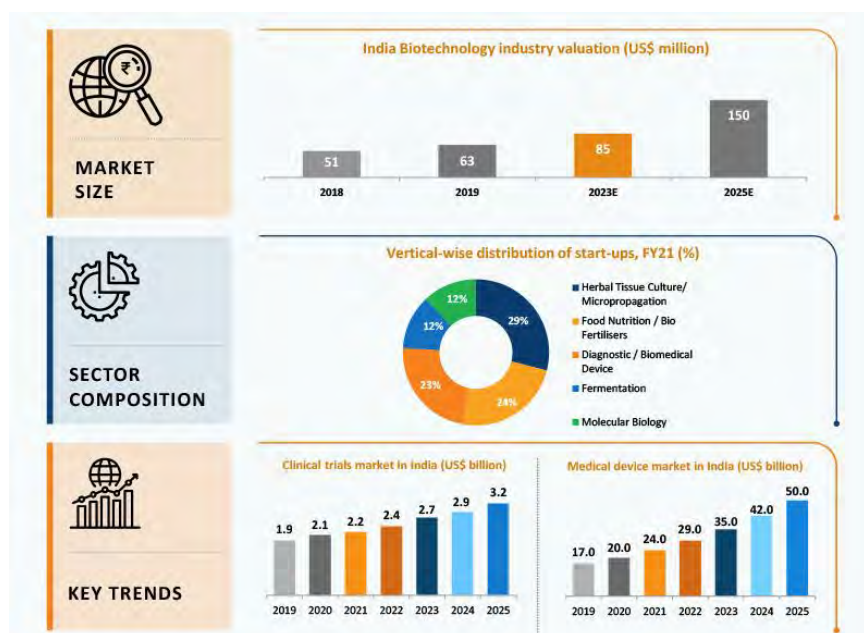


Figure 1 India Biotechnology Market Trends.^M

pandemic/epidemic threats, with no country being 100% prepared.^H In specific areas surrounding political and security infrastructure risk, India decreased 7.2 points, ranking them 110/195.^H These risks are related to internal governmental control measures surrounding biosecurity laws/regulations, training practices and standardization, and personnel vetting with regular security checks. Environmental changes, urbanization, population density, and increased human to animal contact due to these factors increase the risk for natural and zoonotic spread of disease.^H

With India projected to be the most populous country by 2027, rapid transmission of disease from human to human is concerning and makes containment challenging.^H A higher possibility of zoonotic spread of disease in India is possible due to the high density of livestock population and humans.^H Further, reducing the natural habitat for wild animals due to increased human encroachment is a driver of zoonosis.^H Several of the most common zoonotic organisms have treatment or vaccines in place, and the remainder has poor or no treatment or therapeutic prevention methods (i.e., Nipha and Hemorrhagic viruses).^M With the emphasis on preparing for potential future pandemics of unknown etiology, a higher focus is being placed on these pathogens. Due to the high lethality of these diseases, this research requires BSL-4 facilities. Three of India's BSL-4 facilities are located within high density areas ranging from 2.5 to 34 million people making pathogen release a significant risk.^{M,M,M}

India, market leader in BSL 3-4 research facilities, is a prime location for adverse events impacting the region and global population. Experts indicate the security systems and practices surrounding necessary infrastructure to conduct this work safely are lacking. These facilities being located within dense populations, and high pathogenicity of the substances they are working with pose highly lethal consequences if not properly secured.

Analytic Confidence

The analytic confidence for this estimate is *high*. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. An area of concern was the quantifying the accurate number of BSL 3 & 4 laboratories within India with multiple sources offering differing counts. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Medical Implanted Devices Pose Chance of Cyber Security Threat

Executive Summary

More than 400,000 cardiac medical devices are implanted in U.S. citizens annually with the ability to communicate via wireless networks, and limitations in cyber security, these devices have a chance (46-55%) of being hacked by malicious actors causing harm or death to the patients, and striking fear in vulnerable populations. Independent associations and auditors have developed threat models however, the device industry denies vulnerabilities. While not a high volume or high revenue venture for nefarious actors, medical device hacking could prove to be an effective terroristic endeavor.

Discussion

The implanted or wearable medical device market is projected to be \$190B, a 170% increase in five years.^H Since 2007, these devices transmit wireless data to and from the manufacturer and health care providers to enhance care delivery (See figure 1).^{H,H} Technology has steadily improved, and now many devices have smartphone technology capability.^{H,H} Cyber hacking in its modern day construct as well as ransomware attacks have been around since 1989.^M These devices, as well as other types of personal implanted medical devices could be hacked, creating physical harm. Former Vice President Dick Cheney, had the wireless function of his device disabled specifically to prevent an assassination attempt.^H



Figure 1 Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices.^M

There has been rapid growth in the cyber security industry, with the market expected to exceed \$345B by 2026.^M Governmental interest in cyber security increased with the Trump White House publishing a total economic impact being as high as \$109B in 2016.^H Healthcare related cyber security measures are integrated into these figures, with the majority focusing on health informational systems versus personal medical devices.^M Healthcare related cyber security is becoming an area of concern with organizations and associations analyzing threats within the industry.^M The Healthcare and Public Health Care Sector Coordinating Council recently created a Joint Security Plan for information

technology systems but lacked emphasis on personal implanted devices.^H The Joint Security Plan further details challenges to the plan due to “lack of transparency and disclosure between vendors and end users, security by design and throughout the product lifecycle and product end of life.”^H Denoting concern referencing what may be considered proprietary information as it relates to patient safety measures.

The US Food and Drug Administration issued warning notifications regarding specific models of pacemakers and cardiac defibrillators in 2017 and 2019, noting security issues enabling unauthorized personnel to make programming changes.^H While former V.P. Cheney had aspects of his device disabled out of caution in 2013, the concept of hacking these devices is considered theoretical by some experts.^H The devices themselves create unique security challenges that are difficult to overcome, such as lack of memory capacity and computing and authentication measures.^H The devices also remain in the body for years with an average battery life exceeding seven years. If the device cannot be upgraded remotely the only recourse is requiring the patient to undergo another invasive operation to implant a new device.^H

Cyber-attacks have proven profitable for malicious actors predominately at an institutional level. Hacking individual implanted devices is unlikely to generate this same financial benefit. Limitations related to personal medical devices becoming hacked by nefarious actors mean large scale use is not likely. The desired end state of inciting fear within society remains possible. The threat comes from fear and destabilization when a vulnerable population is targeted by terroristic activity.^{H,M}

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Public Health Surveillance Systems Still Not Adequate by 2035

Executive Summary

Despite artificial intelligence (AI) development in health care continuing to expand the delivery of services and public health infectious disease surveillance with the advancement of algorithms, access to quality data, and public integration in platforms, chances are a little less than better (46-55%) AI will offer significant impact to public health surveillance systems by 2035. These systems derived from medical diagnosis, laboratory results, and social media trends have been in existence globally for decades. Leaders in the industry routinely cite the need for advancement; however, challenges surrounding trust and funding make public health surveillance as a biosecurity measure difficult.

Discussion

Artificial intelligence as a construct in the health care industry is gaining momentum. A recent survey indicated that 98% of industry leaders indicated developing an AI strategy



Figure 1 Public Health Components.^M

currently planned within their operational focus.^M The two main challenges from a public health surveillance interface lie between the data sourcing and the analytical processing AI can address.^H AI methods, “particularly those based on machine learning, have long applied to detect patterns, identify anomalies, and analyze trends and risks from

public health surveillance data streams.”^H Therefore, there is anticipated future capability for AI to positively impact health care clinically, as well as preventatively.

Epidemiologic and predictive data has been utilized for decades to ensure public safety. This data, actively and passively obtained via mandatory reporting requirements, is then instituted by local and national agencies.^H Passive data, the most cost-effective and extensive with current technology, does not have robust capability of being predictive.^H Analysis of large quantities of passive digital data for predictive purposes, while broadly cited as necessary, is challenging due to the current ethical and legal constraints of obtaining the data.^M

Digital data systems utilizing platforms such as social media and Google are capable of detecting disease outbreaks and are supplementary to more traditional surveillance methods.^H ProMED reports daily global surveillance data to subscribers, as do systems such as Flu Near You, but both currently lack interoperability to link to other platforms to consolidate information.^{H,M} Crowdsourced systems, while innovative, have ease of use and benefit from global reach, lack specificity, and are dependent on individuals voluntarily inputting data making determinations from the data difficult.^H

Active surveillance systems specifically for bioterrorism surveillance, such as the BioWatch system, intended to sample air for the presence of aerosolized biological agents, were determined in 2009 to need “better technical and operational testing to establish effectiveness.”^{M,M} “It also needs better collaboration with public health systems to improve usefulness.”^H A 2021 audit by the Office of Inspector General found the program severely lacking in capability and capacity and lacked updating since 2017.^H

Dr. Alok Tayi, Ph.D., a life science academic and biotech entrepreneur, stated that public opinion and misinformation about public health measures are ongoing biotechnical threats.^{Annex E} According to recent surveys, public perception of the value of public health and its function increased in 2021, with 71% in favor of increased spending to support programs.^H There remains serious concerns regarding levels of trust in the governmental institutions tasked with implementation and oversight programs.^H Politicization of health care within the U.S. has contributed to the disparity between political parties on whom they trust for medical information. “Republicans being more likely than Democrats (47% to 19%) to say they think the information provided by their state health department about the health of people in their state is unreliable.”^H According to the same study, regardless of the political party, the public views an essential function of public health infrastructure as providing measures to protect against infectious diseases (see figure 1).^H This raises concern regarding the ability of surveillance measures of any variety to have an impact if the public is hesitant to believe the information provided by these institutions.

Funding levels for public health initiatives, including surveillance measures, have reduced over the last two decades. Post 2001, significant attention on public health measures and funding focused on bioterrorism.^H Subsequent attention and funding were also robust during Ebola and Zika virus outbreaks.^H Despite this attention, funding has not been level. “Unfortunately, a pattern has emerged: the country

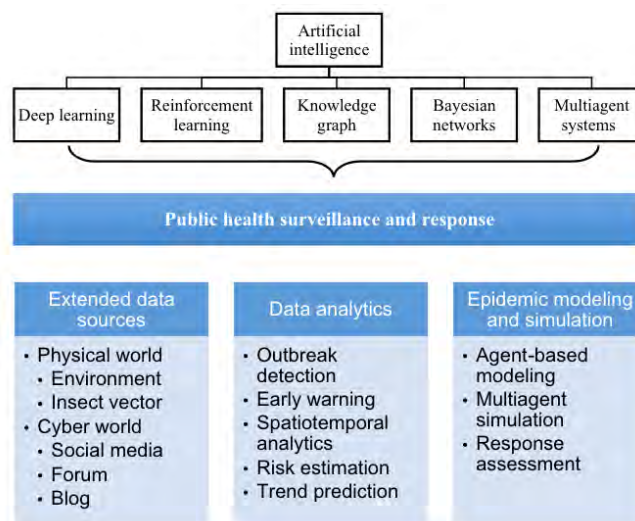


Figure 2 Artificial Intelligence Enabled Public Health Surveillance.^H

temporarily pays attention to public health investment when there is a crisis and then moves on when the emergency passes. This boom-bust cycle has left the nation's public health infrastructure on a weak footing."^H The Centers for Disease Control is an example where public health preparedness and response programs decreased by \$8M between FY2020 and FY2021, and total funds have decreased by half over the past decade.^H Surveillance mechanism in all forms is critical to ensuring public health. Biothreat sensor capability has been met with many constraints, including technical. The ability to interface machine learning/AI will hopefully provide many solutions and opportunities to resolve this issue in the future (figure 2). While the technology is currently in its infancy, there appears to be a focus on its development. The ultimate challenges don't appear to reside in technical capabilities but that of public opinion regarding the data and its analysis by governmental agencies and the lack of resources placed on its development and infrastructure.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were reliable and derived from a cross-section of academic, governmental, and private sector sources. Time for adequate research and reflection were available to the analyst. However, the analyst did work independently with only open-source data for corroboration.

Author: Laura L. Porter

Rapid Tech And Organization Changes Mean Algae Will Likely Be Major Source Of Food By 2035

Executive Summary

Regardless of varying estimates of population growth, climate change and rapid advances in bioengineering, technology make it likely (56-70%) that many countries, particularly in Europe, will develop algae as a primary food source over the next 15 years. Spurred on by the COVID-19 pandemic, all industries are moving to using AI, machine-to-machine communication, and machine learning to reduce manufacturing and personnel costs.^H Despite algae modifying and producing techniques lagging behind in development versus other biotechnological areas, the technologies discussed above can be applied to the coding and categorization of algae genomes, as well as algae production and farming, reducing cost and increasingly the likelihood of algae becoming a staple crop.^H

Discussion

Despite a highly likely (71-85%) flattening of the growth of the world population^H, multiple estimates predict that the global population is still highly likely to reach nearly 9 billion people by the year 2030 barring some unforeseen calamity.^{H,M} The anticipated effects of climate change and continued migrations of populations due to food insecurity will likely be a driver of instability and conflict.^H A shift from unsustainable farming on land could be a solution to these issues.

Microalgae are photosynthetic microorganisms that use CO₂ and light to produce a variety of proteins, carbohydrates, and other microelements such as minerals and vitamins.^H

Microalgae can be grown in

Photobioreactors, which can be as simple as open ponds or various types of glass cases.^H

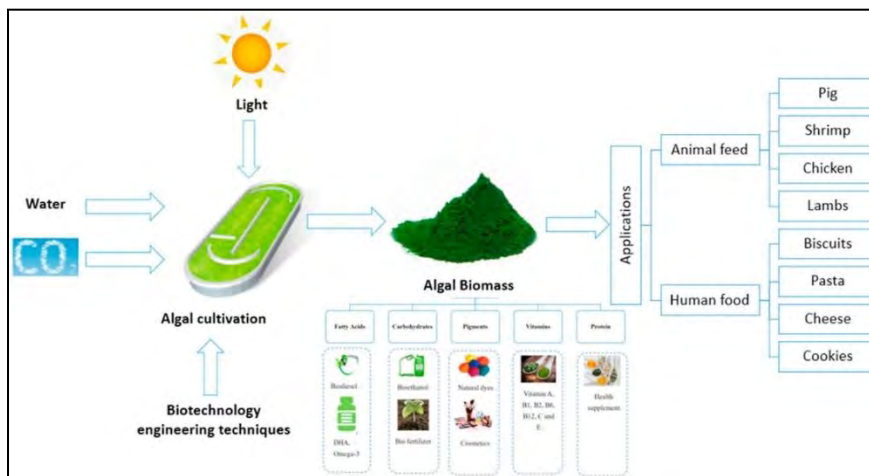


Figure 1 Process of Producing and Converting Algae to Useable Substance.^H

Described as “The 4th Industrial Revolution”, the convergence of physical and digital systems to reduce workforce and increase efficiency has been spurred on by the COVID-19 pandemic.^H The “Internet of Things”, interconnected computers, sensors, and

machines that speed the transmission of data to increase efficiency, is forecasted to increase productivity in factory settings ahead of other areas.^M

If advances in machine learning, machine to machine communication, and artificial intelligence can be applied to algae production, algae's usefulness as a food source can be better realized. These technologies and ideas could be applied to both the bioengineering

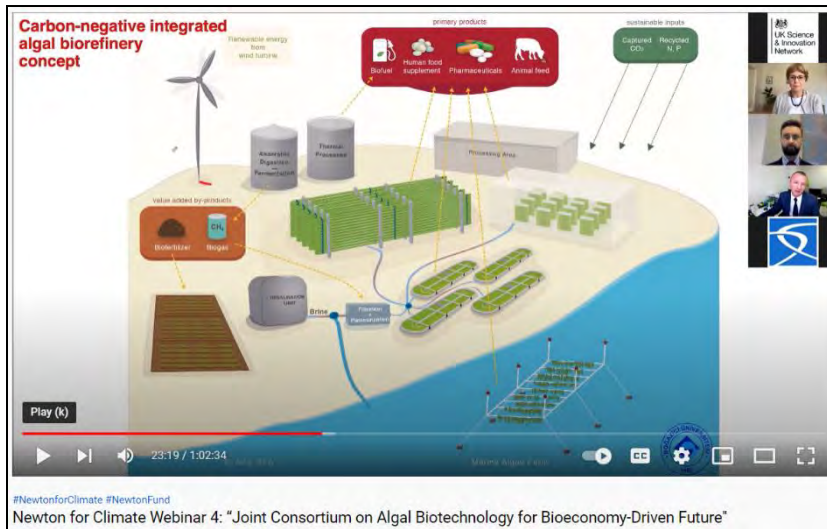


Figure 2 YouTube Video about Project IMBIYOTAB functioning carbon negative algal biorefinery.^H

of microalgae and the physical farming and production of microalgae into foodstuffs.^{M,M,M} This effort has already begun under the auspices of the European Union with their Ocean4Biotech under the European Cooperation in Science and Technology (COST).^H Indeed, The Istanbul

Microalgae Biotechnologies Research and Development Center, Project IMBIYOTAB, has demonstrated the capability to build a functioning carbon negative algal biorefinery (See video link in Figure 2 for a demonstration of this concept).^H

Thus, the convergence of technological, industrial, agricultural, and biotechnological changes make it likely that algae production for food purposes can be realized in light of the societal pressures expected in the next 15 years.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple academic and business sources corroborated the intersection of emerging biotechnology resources and increasing technological changes in industry. There was adequate time to complete the estimate, however the analyst's lack of expertise in the material does not allow for higher than moderate confidence. The lengthy time frame of the estimate means the report is very sensitive to change based off factors beyond technological improvements.

Author: Matthew S. Rasmussen

Another Pandemic Likely By 2035, But Not Due To Accidental Lab Release

Executive Summary

It is likely (56-70%) that there will be another COVID-19 like pandemic by 2035 due to zoonotic transfer from animals to humans rather than accidental release due to poor biosecurity at a research facility. Due to the desire of multiple countries to be prepared for virus outbreaks and to do vaccine research, biosecurity level 3 and 4 facilities will proliferate throughout the world although the biosafety and biosecurity protocols for those facilities will not be regulated or uniform. Despite the risk of “Gain-of-Function” research, the unregulated nature of and expanding footprint of Biosecurity facilities and laboratories, it is unlikely (31-45%) that another COVID-19 like pandemic will occur due to an accidental lab release.

Discussion

Pandemic forecasting has been notoriously difficult. This is due mainly to the intersection of unclear current information during a crisis, social and economic factors, and lack of knowledge of medical infrastructure readiness.^M However, researchers at Duke University analyzing 400 years of pandemic data found that there is a 38% probability that those people living now will experience another pandemic which may double in the coming years.^H Many scientists currently believe that it is more likely (56-70%) that pandemic will come from a zoonotic transfer from animals to humans.^{M,H}

Due to the 2020 COVID-19 Pandemic, interest has grown in the concept of Gain-of-Function (GOF) research. GOF is the concept of involves modifying microorganisms to become more infectious and deadly in order to produce viruses which then allow scientists to engineer vaccines.^H Despite the claim of the 2020 Pandemic being caused by lab research on bats in Wuhan, China, most scientists and the WHO investigation results believe it is highly unlikely (16-30%) that the virus was an accidental laboratory release (see Figure 1).^{H,M} GOF research is a controversial topic as many scientists believe the risks of release of a lethal virus from a lab too high to justify the research.^{M,H,M} Due to this opposition to GOF research, the chances are unlikely (31-45%) that countries will pursue GOF research.

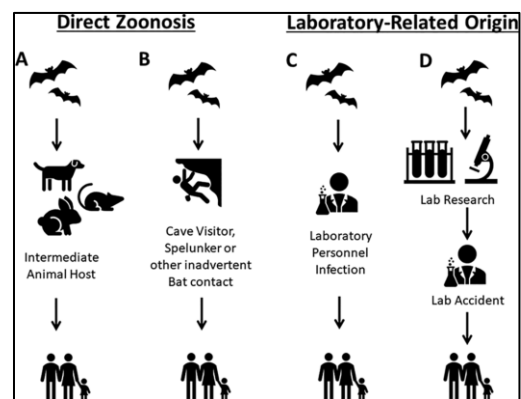


Figure 1 Diagram demonstrating how virus can jump from both animals and laboratory research to create an accidental release.^H



Figure 2 Locations of BSL-4 Facilities worldwide.^M

Also due to the 2020 Pandemic, interest in the facilities where GOF research has increased. Bioengineering facilities are classified in four levels: Biosecurity levels 1, 2, 3, 4; with BSL 1 being the lowest level of security and BSL 4 the highest.^M While the United

States and most European countries have very stringent laws and regulations, other countries do not, or enforcement is likely lax.^M Of the current 59 BSL-4 labs in 23 countries around the world, only 25% of these labs score high for biosecurity and biosafety according to the Global Health Security Index and three quarters of these labs are in urban areas (Figure 2).^{H,H}

However, various countries have demonstrated efforts to reach better biosafety levels. In Egypt and Pakistan training programs to increase researcher awareness of biosafety best practices have increased researcher knowledge and lowered external risk assessments of facilities.^{H,H} So despite the fact that there is no single regulatory body or set of laws or agreements for BSL facilities, the existence of multiple international cooperative agreements and bodies to enforce BSL standards and the movement of individual states towards more safe BSL standards, it is unlikely (31-45%) that a virus will be accidentally released at scale and virulence to cause a pandemic.^H

Taken altogether, the unlikely increase in GOF research, the expanding footprint and semi-regulated natures of BSL-3 and -4 facilities, the location of those facilities, and forecasting on the likelihood of future pandemics leads to the conclusion that it is highly likely that there will be another pandemic by 2035, but that it is unlikely to come from a BSL-3 or -4 facility release.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple academic sources corroborated the estimates of accidental release, the movement towards more biosafety regulations and BSL facilities facts. There was adequate time to complete the estimate, however the analyst's lack of expertise in the material does not allow for higher than moderate confidence. Multiple intersections of scientific research, risk management, human behavior, and animal virus transmission make this estimate very sensitive to change over the time period.

Author: Matthew S. Rasmussen

Advances In Marine Biotech Will Make Weaponized Algae and Toxins Possible, But Unlikely, By 2035

Executive Summary

Algae and marine toxins are unlikely (31-45%) to be a significant threat to the US population by 2035, but could be a threat to deployed forces using local or concentrated water sources. Due to advances in genetic editing and mapping technologies, researchers are highly likely (71-85%) to be able to better manipulate microalgae toxins to combat harmful algal blooms (HABs) which can be lethal to both human and marine life. The same biotechnology could be reverse engineered via “Gain-of-Function” processes to make HABs more lethal and targeted. Largely due to the difficulty in concentrating HAB and toxin effects in the maritime domain and the historically social and political taboos on biological warfare, it is unlikely states will pursue this attack vector against the US homeland.

Discussion

Algae contains some of the most toxic materials found in the world: *cyanobacteria* which produce toxins in warm and stagnant or polluted water. Cyanobacteria in algae can easily move up and down through the water stratification to find the best location for photosynthesis and replicate itself in excess other biological materials in the water.^M When masses of cyanobacteria form together, they can form a

harmful algal bloom (HAB) which have effects beyond the water source where it is formed (see Figure 1).^{H,M} HABs have been known to be lethal to both human and animal life, both marine and land through oral, airborne, and absorption vectors.^{H,M} Current methods of combatting HABs are monitoring and detection. Naturally occurring HABs have effected marine life, local economies, and tourism.

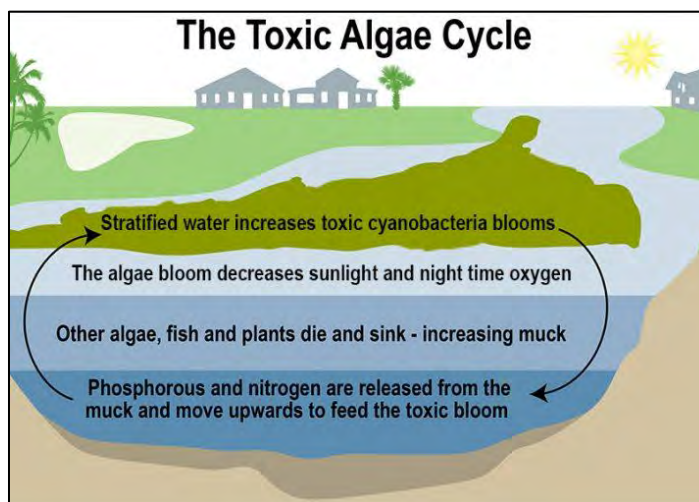


Figure 1 Diagram demonstrating development of harmful algal blooms (HABs).^H

Advances in marine biotech have made it easier to manipulate algae and its associated toxins. Dual use technologies mean that synthetic biology and gene editing could be

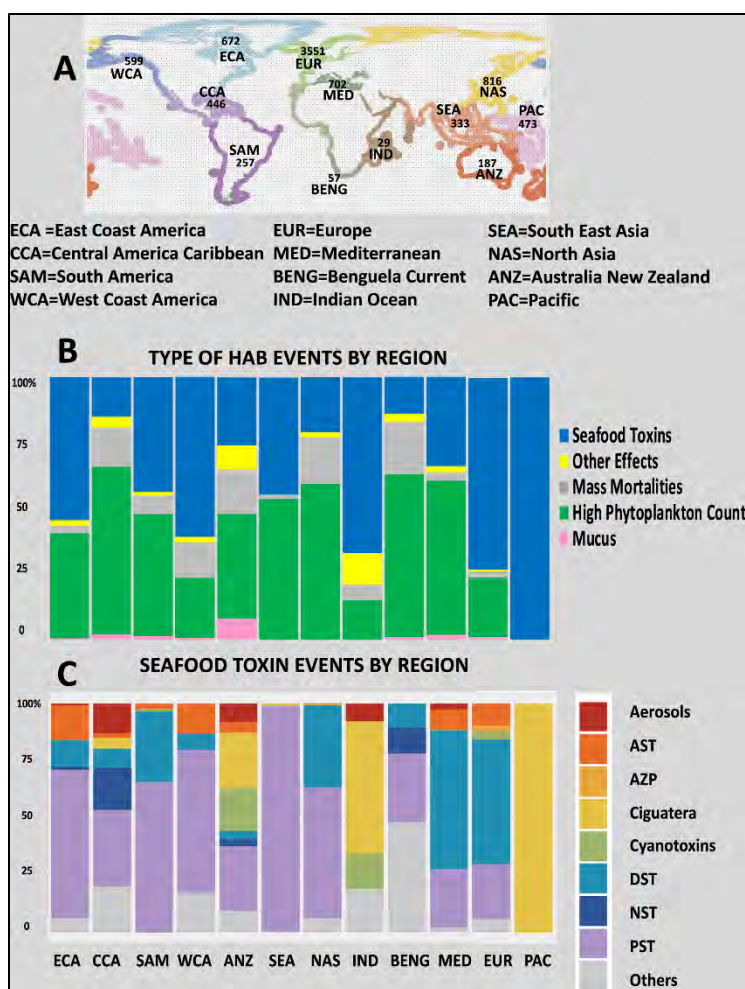


Figure 2 Diagram showing composition of recent HAB and toxin events worldwide.^H

reversed to make well-meaning changes into virulent toxins.^H Other research has demonstrated that using algal chloroplast as a test bed to conduct rapid “design-build-test-learn” can increase effectiveness of synthetic biology making it easier to modify algal toxins.^H It is unclear if the incentive structures exist to push these advances towards wide acceptance by industry or the general population. It is clear that as with most biotechnological innovation, the synthetic biology means to engineer positive changes in algal toxins could be reversed to be negative or deadly.

While HABs have been on the rise naturally (see Figure

2), the natural effects of HABs have not risen to a level of severity that has caused catastrophic human losses, either through direct poisoning or contamination of food or water supplies. Since World War I, long standing political and social norms against the conduct of biological warfare has made it unlikely (31-45%) that states will deliberately employ bioengineered biological weapons. Thus, though capable to, most states will most likely not resort to using HABs or algal toxins on a large scale. There does remain a threat on a lesser scale of a non-state actor using this attack method on a localized water or food supply. Non-state actors could, with current technology, bioengineer toxins which could cause damage or injuries. With the spread of synthetic biology technologies and lower barriers of entry, it is likely (56-70%) that non-state actors could develop bioengineered marine toxins and target smaller, local facilities and supplies.^H

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple academic resources confirm the ability to and interest for increased marine biotechnological research towards

practical application. There was adequate time to complete the estimate, however the analyst worked alone with a general lack of expertise. The lengthy time frame of the estimate means the report is sensitive to change based off factors such as economic shifts in the agricultural and industrial base.

Author: Matthew S. Rasmussen

U.S. Highly Likely To Maintain A Competitive Advantage In Biotechnology Through 2035

Executive Summary

Despite many countries investing heavily into biotechnology, it is highly likely (71-85%) the United States will maintain a competitive advantage across the biotechnology industry through 2035. An analysis of the largest 376 publicly traded biotechnology companies in the world illustrates that due to the value and quantity of companies in the United States, future market projections favor the U.S over its competitors like China.

Discussion

Market capitalization, or market cap for short, “is one way of evaluating the value and size of a company from the point of view of an investor.”^M While it is a “perceived value” of a company at a given time based on the number of shares and trading price, it does serve as a good indicator of stability.^M Large cap companies tend to weather financial storms better than smaller cap companies.^M Additionally, investment is critical because it provides “companies access to the vast amount of cash necessary to advance.”^M Starting in 2013 biotechnology benefitted from “public investment...pouring into the industry.”^M Although, this has fallen off some, market cap is a valid and fundamental metric to evaluate the prospects of a company and the biotechnology industry as a whole.^{M,M}

The U.S. leads in world market capitalization (See Figure 1).^M The list included 23 countries with one or more companies making the top 376. As of 21 March 2022, the approximate total market cap for all U.S. companies on this list is around \$2.9 trillion or 60% of the overall \$4.9

| Rank | Country | # of Companies | Market Cap |
|------|---------------|----------------|------------|
| 1 | United States | 277 | \$2,9587B |
| 2 | Switzerland | 8 | \$592B |
| 3 | UK | 13 | \$342B |
| 4 | Denmark | 5 | \$276B |
| 5 | France | 3 | \$131B |
| 6 | China | 7 | \$127B |
| 7 | Germany | 7 | \$115B |
| 8 | Japan | 3 | \$107B |
| 9 | Australia | 4 | \$95B |
| 10 | India | 9 | \$64B |

Figure 1 Top 10 Countries By Market Cap From The 376 Largest Publicly Traded Biotechnology Companies.^M

trillion represented. Switzerland is the next nearest competitor with an estimated market cap of \$592 billion or 12% of the given market. The next 8 countries to complete the top 10 are the United Kingdom, Denmark, France, China, Germany, Japan, Australia, and India in that order. These countries range from around 7% of the market considered down to a low of 1% for India.

Another useful statistic to consider is the number of companies by country that made the top 376 list. As expected, the U.S. has the majority with 277 or 74% of the companies on the list, while the next nearest country is the United Kingdom with 13 companies. The quantity of companies in each country measures the amount of competition in the market. By this measure and coupled with the value of these companies, it is reasonable to expect more innovation in biotechnology to come out of the US than anywhere else in the world. As an example, the US response to COVID-19 utilizing Operation Warp Speed demonstrates its ability to “leverage the world’s most innovative private [biotechnology] sector” to address a global challenge.^M

As the public, or government sector, often hides their discoveries, the private sector moves theirs to market quickly. As an example, in the U.S. and Europe biotechnology investments are roughly 80% private sector and 20% government.^M The question remains if these percentages hold true in authoritarian countries like China or whether those governments are investing a higher percentage in the government biotechnology sector compared to the private sector. In 2021, China spent roughly \$621.5 billion on Research and Development (R&D) across all sectors outspending the U.S. who spent \$598.7 billion.^M Despite these figures, an independent analysis noted that “the lack of independent innovation capabilities of China’s biotechnology sector restricts the sector’s development.”^M Again, this illustrates the value and need for a healthy private biotechnology sector to effectively position a Nation on the cutting edge.

A Polaris Market Research report published in December 2021 predicts a similar favorable U.S. outcome based on potential market size, or maximum number of sales, as compared to the rest of the world.^{M,M} Additionally, the report valued the global biotechnology market size in 2021 at approximately \$1 trillion dollars with an expected annual growth rate close to 16% across “six major areas, including biopharma, industrial, agricultural, food, environmental, and bioinformatics” with a strong U.S. majority.^M

Based on current market capitalization and future projections, it is highly likely (71-85%) that the U.S. will maintain a competitive advantage in the biotechnology industry through 2035. However, as the world continues to become more interconnected combined with foreign investment, adversary countries like China will seek to exploit the U.S. free market and the intellectual property that comes with it.^M Given most advanced biotechnology discoveries are dual use, the U.S. must work to guard intellectual property going forward or risk an adversary turning U.S. innovation against itself.^M Additionally, as DoD works with private industry to develop biotechnology capabilities, protocols to protect military advancements are critical.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst had adequate time, but the task was complex. The amount and reliability of sources available on the economics behind the biotechnology industry was vast and often contradictory. Additionally, since this estimate focused primarily on the private sector, gaps in the public sector remain. Most sources available did corroborate each other regarding the US as the current leader in the biotechnology industry. Analyst collaboration was modest.

Author: Timothy A. Harloff

Nanomaterials Highly Likely to Increase Food Production Over the Next Decade

Executive Summary

The use of nanotechnology (nanos) in agriculture is highly likely (71-85%) to increase food production in the next ten years due to proven benefits in pest reduction and increasing crop yields. However, as scientists make advances across multiple applications, the potential for unintended consequences rises in crop reduction or elimination, or other dangers such as unknown environmental impacts, creating high levels of toxicity in plants, humans, and animals. Additionally, adversaries might weaponize nanos to kill crops and destroy food supplies which is challenging to detect. Developments in nanos like Silica Nanoparticles (SNPs) and Carbon-based Nanomaterials (CNMs) can also influence medical, industrial, military, and aquatic biotech areas. A threat is the inability to feed troops due to loss of food supplies from weaponized nanos.

Discussion

Nanotechnology, characterized by small particles ranging from 1 to 100 nanometers is ready for exploitation and growth in the agricultural sector.^H Nano opportunities and applications span biological pesticides, nucleic acid pesticides, plant growth regulators, chemical pesticides, pheromones, and fertilizers (See Figure 1).^H By 2050, food production will need to increase by 60% to feed the estimated growth in the world's population.^H Research from the Toxicology and Applied

Pharmacology Journal states, Nanos will likely positively impact environmental challenges and improving the use of resources.^H Still, adversaries are likely to utilize nanos to impact the environment to attack food security.

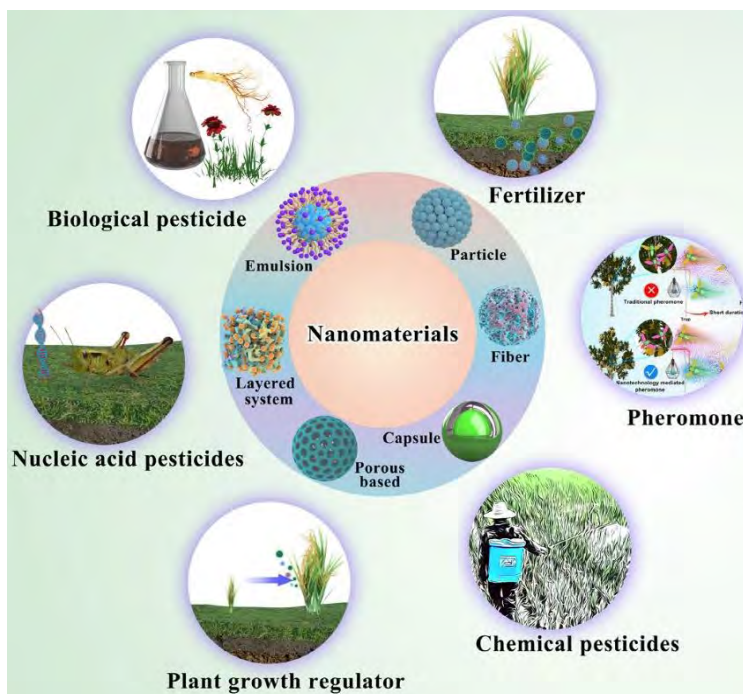


Figure 1 Nanomaterials Loaded with Various Agrochemicals Enabling Nanoparticles to Adhere to the Target to Improve the Bioavailability of Active Ingredients.^H

Silica Nanoparticles (SNPs) are promising nanotechnology with the potential for weaponization. They help with plant growth and are useable as nanopesticides, nanoherbicides, and nanofertilizers.^M Chinese scientists state, "The applications of silicon and SNPs reduce the oxidative stress response by priming defense reactions under biotic and abiotic stresses."^M Combining SiO₂ with cellulose (Silica biofiber) can slowly release nitrogen fertilizers, increasing rice crop chlorophyll content.^H The absorption and transmission of SNPs in plants are beneficial due to their small size and ability to transit cell walls. However, there is a lack of research on follow-on impacts to the plant and environment.^M Competitors might exploit SNPs to mask the delivery of harmful chemicals or pathogens that slowly leach into the environment or a host making it hard to detect.

Carbon-based nanomaterials (CNMs) usage is growing more common.^{H,H} Combining CNTs, graphene, and zinc ferrites (ZnFe₂O₄) nanos resulted in an effective super fertilizer resulting in significantly better plant growth, with less pollution and reduced harmful chemicals.^H Chinese scientists in the *Plants Journal* state, "There is an urgent need to understand how plants respond to their exposure. Moreover, the addition of CNMs has increased the complexity of the agro-ecosystem; whether they represent a new pollutant or a new opportunity" is to be determined.^H Adversaries might utilize CNMs to develop means to deliver pathogens or toxins into the environment or humans.

Future research in nanotoxicology in agriculture is needed to better understand the impacts of nanomaterials' entire spectrum. A recent discussion with Dr. Alok Tayi, the co-host of the BioTech 2050 Podcast, discussed the absence of understanding of toxicity in the biotech continuum.^M Scientists must know more about "the interaction mechanisms of a nanostructured material with a living organism (plants, animals, or even human beings)."^H Metal Oxide nanos are a promising area in agriculture as a possible shield against arsenic toxicity. However, different concentrations of the nanos determine the benefit or damage to plants.^H Another promising area of study is the convergence of machine learning and monitoring the absorption of engineered metallic nanos.^H Competitors using similar technology might gain insights on the needed thresholds to kill crops and significantly impact food availability.

Future challenges and dangers to humans and the environment exist with nanotechnology in agriculture and other uses. Toxicology scientists stated, "New environmental and human health hazards may emerge from nano-enhanced applications. This raises concerns for agricultural workers who may become primarily exposed to such xenobiotics during their job tasks."^H Government environmental safety assessments, policies, and oversight of the nanomaterial industry will enable a more safe and sustainable food supply and environment.^H

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Justin L. De Armond

Biosurfactants Likely to Reduce Threats and Improve Biosecurity By 2035

Executive Summary

Biosurfactants are likely (56-70%) to reduce toxins, toxicity, and pathogens throughout the agro-environment and other industries, improving food security in the next ten years. Despite 40 years of biosurfactant research, the scientific community is ramping up efforts to utilize biosurfactants in agriculture, pharmaceuticals, industrial, and environmental remediation.^H Utilizing bacteria and nanoparticles to develop remediation and antimicrobial capabilities will help reduce current harmful synthetic surfactant practices. Competitors might use synthetic surfactants that are themselves harmful or protect dangerous substances using biosurfactants and enable their delivery into the food system leading to food insecurity. Agroterrorism is a potential threat, and biosurfactants are just one solution to addressing potential contamination issues.

Discussion

Fifteen million tonnes of surfactants, which are highly toxic and do not biodegrade, enter the environment each year, increasing the need for biosurfactants, but low production yields slow industrial development.^{H,H} The biosurfactants annual market is over \$5B, roughly

10% of the total \$41B surfactant market.^{M,M} As demand for green solutions drives the industry's growth, biosurfactants are likely to lead the transition away from more harmful synthetic surfactants to protect living organisms and industry. Biosurfactants have multiple agricultural applications from soil improvement, pathogen elimination, seed protection and growth, use of biopesticides, increased microbe interaction, and enhanced nutrient availability (See Figure 1).^H

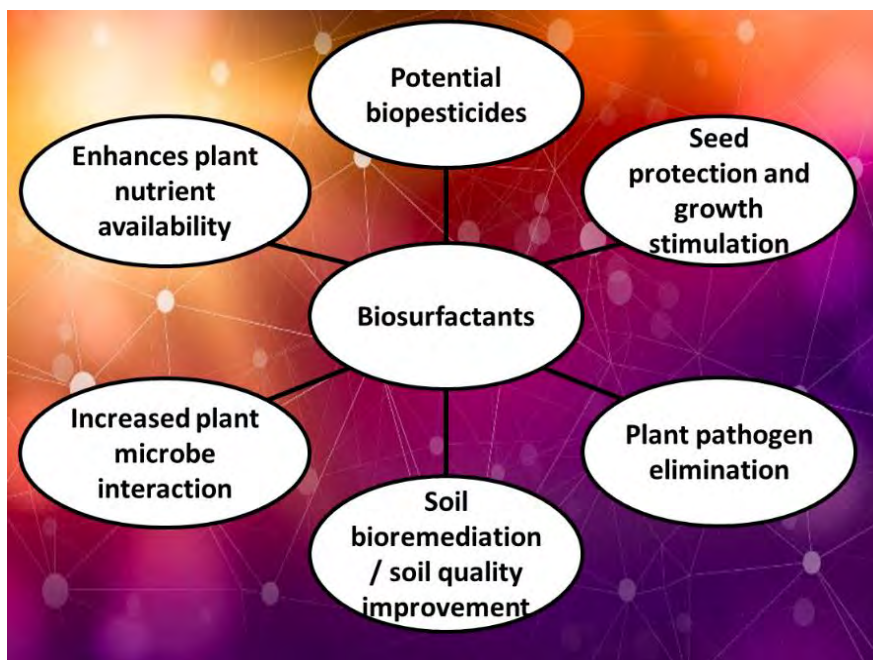


Figure 1 Potential application of biosurfactants in agriculture.^H

Eliminating plant pathogens is a significant future research concern for biosurfactants as natural and human-introduced diseases can degrade food security. An area of study to reduce disease is using rhamnolipids or lipopeptides. Rhamnolipids are biosurfactants that can eliminate plant pathogens.^{H,H} Agricultural industry waste can produce biosurfactants that are reciprocally beneficial to the remediation of soils.^H Biosurfactants are helpful as emulsifiers, preservatives, and antioxidants in the food production process.^H Phytoremediation, in conjunction with plant growth-promoting rhizobacteria (PGPR) and rhizobium, enables heavy metal phytoextraction.^H *Rhodococcus opacus* R7, is another biosurfactant with promising antimicrobial results and degradation of naphthalene (a volatile, solid polycyclic hydrocarbon) that show potential in the biomedical, food industry, pollutant removal, and biotech fields.^{H,H} Biosurfactants might protect the Army's food supplies from natural and enemy toxins and pathogens.

Combining biosurfactants with other materials such as nanoparticles will aid the agricultural industry by removing oils, pathogens, and toxins from the soil. Without remediation, the use of organic pollutants in the agriculture and industrial sectors has negative impacts on human health and the entire ecosystem.^H Researchers utilized iron and copper nanoparticles combined with rhamnolipid and sophorolipid biosurfactants to remove petroleum hydrocarbons from the soil.^H The challenge is producing enough biosurfactants to address areas of contamination. Additionally, the soil must be removed and processed to have the most impact.^H Enhanced soil washing using rhamnolipid is an efficient and cost-effective method to remove heavy metals (cadmium) and oil (phenanthrene).^H Adversaries might attack oil infrastructure, impacting an agricultural region or drinking water source. However, cleaning contaminated areas using biosurfactants with nanoparticles is possible.

Potential threats emerge from the massive amounts of synthetic surfactants produced and used each year. The main issues arise as synthetic surfactants find their way into the soil, water, and daily use products. Water quality, in particular, is of concern as surfactants can easily enter the human body and have toxic effects.^H Additionally, synthetic surfactants reduce available oxygen in water harming marine life, but also increase toxins in the aquatic environment and can reduce plant photosynthesis processes.^H Detection of synthetic surfactants, along with heavy metals, oils, pathogens, and other toxins, must be a priority to ensure food security and might protect Soldiers and their equipment in a contested environment. Biosurfactant discoveries are enabling future research opportunities in all fields of biotechnology. Scientists from the University of Minnesota are learning more about lung surfactants that might lead to better treatments for respiratory illnesses.^H

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources are reliable and tend to corroborate one another, but the original sources used to compile the accessed reports

were not always available. There was adequate time, but the analyst is not an expert, worked alone, and did not use a structured method. Furthermore, given the lengthy time frame of the estimate and its reliance on new biosurfactant research, this report is sensitive to change due to new information.

Author: Justin L. De Armond

Annexes



BIOTHREAT
FORGE

Annex A – Terms of Reference

Terms of Reference: *Expected Biothreats 2035*

For:

**Mr. Jeffrey Singleton
Deputy Assistant Secretary of Defense for Research and Technology
(DASA R&T)**

By:

**Team Biothreat Forge
U.S. Army War College (USAWC)**

December 16, 2021

Terms of Reference:
Biothreats 2035

Requirement:

What surprising biotech capabilities will potentially threaten U.S. people, infrastructure, and/or the military by 2035?

Sub-questions:

- What are the most likely U.S. resources (people, infrastructure, organization, etc.) a group would likely target with a biologically based technology?
- What areas of biotech are adversaries developing threats?
- What current or emerging technology could be used to engineer or deliver a biothreat with limited resources?
- Are the developing biotech capabilities reproducible at a small scale, with commercially available resources?
- What biological processes are being used/developed that could pose a be weaponized by 2035?

Methodology:

The team intends to gather information through a variety of means, including but not limited to data collection from open-source outlets and interviews with biotech academia, think tanks, private and public laboratories, biotech area experts. Subject areas include but are not limited to bioinformatics, medical, industrial, agricultural, and environmental. Then the team will evaluate how various biotechnology could be used to threaten resources within the U.S. The **intent isn't to develop enemy courses of action, rather it is to determine** what is in the art of the possible. Finally, if in the course of research the team discovers any significant opportunities for biotechnology use in the Department of the Army, then the team will highlight these during the outbrief, but this is not the focus on **the team's research.**

In-Scope:

- Attempt to focus on identification of emerging areas not currently considered, i.e. **“blind spots” in current thinking**
- Creative, non-concordant thinking
- Timeline: viable around 2035

Out-of-Scope:

- Offensive measures the United States can utilize against adversaries
- Ethical considerations/limitations – not a restriction for our enemies
- Budgetary constraints for development

The team will conduct our research in several phases:

- Gather Information (November 2021 – February 2022):
 - Each group member will do broad based open-source research into a specific topic area to develop a greater understanding of that area.
 - Evaluate the most likely areas of biotech adversaries might be used to target the United States
 - Connect with biotech and other industry experts to assess biotech **threats against multiple different physical systems in today's modern world**
 - Assess the developing biotech ideas and science to understand better potential threats and their timelines to use against US capabilities and resources
 - Explore all emerging aspects of biotech and the potential to turn new capabilities into possible threats
 - Research biotech raw materials, deployment and tracking of resources to aid in protection discovery
 - All research will be available to all team members using a knowledge management program, such as Zotero.
- Analysis and Synthesis (February – March 2022):
 - During this phase the team will evaluate all the research and determine what biotechnology has the greatest potential to be weaponized against the U.S.
 - Team will use a qualitative scoring system and possibly use a pairwise comparison to evaluate biotechnologies against each other to determine the top threats.
 - Emphasis will be on biotechnology that is either ubiquitous or available with limited resources. The intent is to prioritize threats from non-state actors or from state backed actors that may be attempting to hide their involvement.
 - Comparison between biotechnology and targets will be useful in this phase.
- Compile concepts and prepare report (March – April 2022):
 - **Compile a comprehensive report of the team's findings**
 - Develop a presentation and supporting materials to deliver and out-brief to Mr. Singleton.
- Out-brief Mr. Singleton and team (May 9-13, 2022)

Challenges:

The team's expected challenges include:

- Continued academic requirements from USAWC core courses.
- Potential COVID-19 restrictions.
- Biotechnology is a vast subject area; we may give an incomplete answer in the time allotted.
- Access to proprietary data/information, research labs, think tanks, and subject matter experts.

- No expertise in biotechnology on the team.
- Creativity and imagination of team members.

Resources:

- The team will utilize the US Army War College databases and resources and other commercial and educational resources available.
- The team will utilize open-source media and published information from academic and professional institutes.
- The team will identify and connect with government, international, academics, laboratories, think tanks, and private biotech subject matter experts.
- The team will target and attend professional conferences, conventions, and/or seminars related to biotech as appropriate.
- The team is comprised of Army officers with diverse backgrounds.
- The team will leverage personal and professional relationships with domestic and international colleagues spanning military, government, academic, organizational, and institutional entities.

Administration:

- The final product will be provided in PDF format and is for the sole use of Mr. Singleton, DASA R&T and for those he so designates.
- The draft outbrief will be ready for presentation upon completion of peer-review, with final outbrief May 2022.
- The research team includes:
 - Team Point of Contact:
 - COL Dan Mitchell; daniel.mitchell.mil@armywarcollege.edu; 931-436-3226
 - Alternate Team Point of Contact:
 - COL Laura Porter; laura.porter.mil@armywarcollege.edu; 919-906-9933
 - Team Members:
 - LTC Tim Harloff
Timothy.harloff.mil@armywarcollege.edu; 334-447-9618
 - LTC Justin De Armond;
Justin.dearmond.mil@armywarcollege.edu; 256-479-6040
 - LTC Matt Rasmussen;
matthew.rasmussen.mil@armywarcollege.edu; 706-718-8677
- Official Mailing Address: COL Dan Mitchell, c/o Army War College, 100 Forbes Ave, Carlisle, PA 17013

Annex B – Assessing Analytic Confidence

The analysts were not subject matter experts and some topics required extensive scientific knowledge to fully grasp. The analysts worked independently and collaboratively to answer the question. They utilized a combination of structured analytic techniques including nominal group technique and network analysis. The team evaluated their analytic confidence using Peterson's Analytic Confidence Factors coupled with the Friedman Corollaries.

Peterson's Analytic Confidence Factors

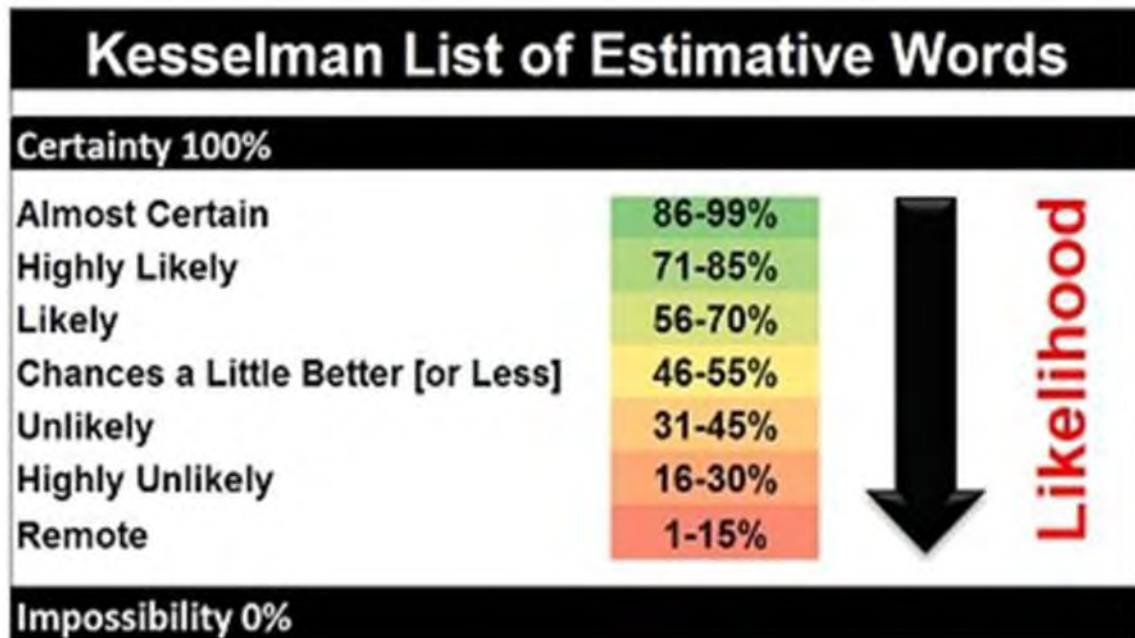
- How reliable are the sources?
- How well do the independent sources corroborate each other?
- What is my/my team's level of expertise?
- How effective was my analytic collaboration?
- Did I use any structured techniques in my analysis?
- How difficult did I perceive the task to be?
- Did I have enough time to complete the task?

Friedman Corollaries

- Is my estimate within the range of reasonable opinion surrounding the question?
- How likely is it that new information will change my estimate?

Annex C – Kesselman List of Estimative Words

Team “Biothreat Forge” utilized the Kesselman List of Estimative Words as their Words of Estimative Probability (WEP) for determining the likelihood of a biotechnology capability to threaten U.S. people, infrastructure, and/or the military by 2035. Analysts used these WEPs in individual estimates of specific threat capabilities, as well as in the analysis of the biotechnology trends towards 2035.



Annex D – Source Reliability

Analysts note source reliability at the end of each citation as low (L), moderate (M), or high (H). The citation was directly hyperlinked to the open-source content at the time the analyst produced the estimate. Team “Biothreat Forge” determined source reliability using the Standard Primary Credibility Scale and the Trust Scale and Website Evaluation Worksheet. Figures and photos embedded throughout this document are also hyperlinked to their source.

| Standard Primary Source Credibility Scale (“The Paul Scale”) | | | |
|---|--|--|---|
| <u>Importance</u> | <u>Factor</u> | <u>Description</u> | <u>Satisfies Criteria (Yes /No)</u> |
| HIGH | Has a good track record | Source has consistently provided true and correct information in the past | |
| | Information can be corroborated with other sources | Information provided by the source corroborates with information from other primary and/or secondary sources | |
| | Information provided is plausible | High probability of the information being true based on the analyst's experience of the topic/subject being investigated | |
| | Information is consistent and logically sound | Information provided is consistent when queried from different angles and is logically sound | |
| | Perceived expertise on the subject | Source is perceived to be an expert on the subject / topic being investigated and/or is in a role where subject knowledge is likely to be high | |
| | Proximity to the information | Source is close to the information – a direct participant or a witness to the event being investigated | |
| | Perceived trustworthiness | Source is perceived to be truthful and having integrity | |
| MEDIUM | No perceived bias or vested interest in the subject / topic being investigated or on the outcome of the research | Source has no perceived bias or vested interest in the subject / topic being investigated or on the outcome of the research | |
| | Provides complete, specific and detailed information | Information provided is specific, detailed and not generic | |
| LOW | Is articulate, coherent and has a positive body language | Source is articulate, coherent, has a positive body language and does not display nervousness or body language that can be construed to be evocative of deceptive behavior | |
| | Recommended by another trusted / credible third party | Source is recommended by others the analyst trusts but the analyst herself does not have any direct experience working with the source | |
| | Sociable | Source comes across as outgoing and friendly. Easy to get along with and talk to | |
| | Perceived goodwill to the receiver | Perceived intent or desire to help the receiver or the analyst | |

| Trust Scale and Web Site Evaluation Worksheet (Updated OCT 2013) | | | | | | | | | | | | | | |
|---|--|-----------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|---------------------|
| Piece of Evidence #: | | | | | | | | | | | | | Score: | Trust Scale: |
| Criteria | Tips | Value | Y or N | Y or N | Y or N | Y or N | Y or N | Y or N | Y or N | Y or N | Y or N | Y or N | 0 | 15-20 High |
| Content can be corroborated? | Check some of the site's facts | 2 | | | | | | | | | | | | 11-15 Moderate |
| Recommended by subject matter expert? | Doctor, biologist, country expert | 2 | | | | | | | | | | | | 6-10 Low |
| Author is reputable? | Google for opinions, ask others | 2 | | | | | | | | | | | | 5-0 Not Credible |
| You perceive site as accurate? | Check with other sources; check affiliations | 1.5 | | | | | | | | | | | | |
| Information was reviewed by an editor or peers? | Science journals, newspapers | 1.5 | | | | | | | | | | | | |
| Author is associated with a reputable org? | Google for opinions, ask others. | 1.5 | | | | | | | | | | | | |
| Publisher is reputable? | Google for opinions, ask others. | 1.5 | | | | | | | | | | | | |
| Authors and sources identified? | Trustworthy sources want to be known | 1 | | | | | | | | | | | | |
| You perceive site as current? | Last update? | 1 | | | | | | | | | | | | |
| Several other Web sites link to this one? | Sites only link to other sites they trust | 1 | | | | | | | | | | | | |
| Recommended by a generalist? | Librarian, researcher | 1 | | | | | | | | | | | | |
| Recommended by an independent subject guide? | A travel journal may suggest sites | 1 | | | | | | | | | | | | |
| Domain includes a trademark name? | Trademark owners protect their marks | 1 | | | | | | | | | | | | |
| Site's bias in clear? | Bias is OK if not hidden | 1 | | | | | | | | | | | | |
| Site has professional look? | It should look like someone cares | 1 | | | | | | | | | | | | |
| Total | | 20 | | | | | | | | | | | | |

19 Dec 2001: The criteria and weighted values are based on a survey input from 66 analysts. For details see: <http://daxnorman.googlepages.com/analysis>. Edited for simplicity by Kristan J. Wheaton, OCT 2013
 3 Feb 2012: Excel Spreadsheet which adds auto-sum was produced by Bill Welch, Deputy Director, Center for Intelligence Research Analysis and Training, Mercyhurst College.
 26 Jan 2013: Trust Scale and Web Site Evaluation Worksheet is in the PUBLIC DOMAIN.

Annex E – Interview/Communication Notes

Interview Notes

Collaborative Meeting Notes 26 JAN 2022 @ 1130

LTC Jarod Hanson, USAMRIID XO

MAJ James Kluckman, USAMRIID

COL Dan Mitchell, COL Laura Porter, LTC Matt Rasmussen, LTC Tim Harloff,
LTC Justin De Armond, Mr. Fred Gellert

COL Dan Mitchell

Team Biotech Forge met with COL Jarod Hanson and MAJ Jeffrey Kluckman from USAMRIID on 26 JAN 2022 to discuss the work done there and gain a greater understanding of potential biothreats of the future. COL Hanson and MAJ Kluckman seemed like true experts in their fields. This discussion lasted approximately 90 minutes and was very productive at identifying current efforts and gaps.

The following is a series of notes from this discussion, not necessarily in order but more or less grouped into similar categories. These are not comprehensive and likely only reflect my research interests.

Labs like USAMRIID (BSL 3 facility): This is one of the most capable labs in the country, second only to the CDC. There are many agencies and other DoD working here (post-BRAC) and they support OGAs with their research. If Hanson and Kluckman (H&K) are any indication then it's likely that this location employs only top notch researchers.

- Aberdeen CCDC
- CDC (BSL 4)
- Rockymount
- Medical Research lab in Galveston, TX
- DITRA

H&K indicated that all BSL 3 & 4 facilities will have/had a 'leak' at some point. Each country has their own regulations, inspections, and enforcement mechanisms and these standards are not regulated across the world by any one organization like the WHO, UN, etc. H&K indicated that there are many other BSL 3 & 4 facilities being built around the world and this potentially a problem for leaks of nasty stuff (paraphrase mine). These facilities are very energy intensive; they may look different but will draw lots of power.

Equipment/Resources/Education/Training needed to do make nasty stuff:

- H&K indicated this entirely depends on your risk tolerance and what bug you're working with
- Minimum needed is a facility that is warm enough to incubate a cell culture
- Old School techniques are still very relevant (incubation in pigs and mice brains) to growing a bioterror
- Gene Synthesizers are increasingly more available and prices are currently in the \$50-60k range but will be 10x less by 2035 (estimate)
- Gene synthesizers can make a 'bug' in as little as 2-3 days, then it needs a few weeks to incubate and rescue/harvest
- Advances in Cell Free systems will make 'bug' production easier <<this means that labs will be able to synthesize a cellular environment without having an actual cell>>; 5-10 year timeline
- All gene sequences are available on open source databases
- It's possible to order 'toothless' bugs (pox, etc.) from commercial companies; these can be modified in a home lab to make them dangerous again
- Education requirement baseline is a 1st year PhD microbiology student; however, an undergrad who has worked with a PhD can have the skill sets necessary to do gene editing
- Naturally occurring 'bugs' are available in the open environment, such as H5N1 Flu, and can be made more dangerous in a home lab

Gaps:

- Toxin research: all but discontinued by the government
- Bio surveillance (huge gap):
 - Sensor field reliability
 - Results review to separate the wheat from the chaff
 - AI can make this better but it will be hard to train the AI to do this effectively
- Preons like Mad Cow are not heavily researched/tracked
- Methods to control a biological outbreak
 - If you can immunize your population before you release a bug, you're more likely to use the bug
 - China is far ahead of the US on Human Genome Modification (embryo, HIV)
- Plant Pathogens
- Delivery systems:
 - insect, plant
 - person to person from people 'outside the system' like the homeless

COL Laura Porter

Background

USAMRIID - no longer focuses on Offensive medical warfare - only defensive. Primary focus prior to COVID was not on diseases of public health. Focus is on

countermeasures and serves as a training center for other labs. Research is driven by payor sources with the majority being grant-funded/DHA... The term utilized was "fully reimbursable lab".

They are partnering with 8-9 other BSL4 Facilities. DoD - Navy BSL3, Chem Bio Defense labs. CCBC at Aberdeen. Peer - are a backstop to the CDC. 3 CIV comparable labs Rocky Mountain Lab, a Lab in TX, and an additional one. However focus is not geared toward offensive countermeasures. Private sector has a bias against assuming something is nefarious.

Countries known to be working in this area biotech/biodefense +/- bioweaponry: Russia, Germany, France, UK, China, Canada, North Korea

Ease of Development

Production can be easy if you have a high tolerance for Risk - if high tolerance you need very little infrastructure support and elements can be obtained easily on the commercial market. i.e. H5N1 can be grown in a garage.

Educational prep PhD student easily, undergrad w/ lab experience can accomplish. A Post Doc Grad student synthesized Horse pox via reverse engineering out of a traditional lab.

Instructions on how to grow bacteria/virus "recipe books" all public/open source.

Technology

- Gene fragment synthesis - infrastructure less than a size of a toaster, and costs around \$50K - can print full RNA/DNA and do it in a couple of days to weeks.
- Use of AI is already occurring to make things faster.
- Using bioweapon current challenge is if you "pull the pin" you cant control it. What will change will be the application of control measure to the population to effect/not effect as desired "Human Genetic Modification" "Modification of the Host" "Ways to control the target"

Gaps in thinking/research

- Cell Free Technology systems - can be developed without cell culture capability
- Virus Propagation - mouse cerebral sample. Undetectable by vendor driven entities.

- "Biosurveillance is a big gap". Liabilities: Highly unreliable in field settings and need a competent reviewer to analyze/interpret data. Assays are Agnostic - Highly sensitive not specific
 - Prions
 - Toxin research - Marine Toxins
 - Recombinant Virus
 - Insect borne diseases
 - Plant based (banana) pathogens
- Keep it simple - what is common can be catastrophic. The easiest transmission is still host to host/person to person.

LTC Matt Rasmussen

Biosecurity Level (BSL) 3 & 4 Labs

- Infrastructure
 - Extremely energy intensive
 - What future tech could produce more energy at lower space and cost and be combined with a BSL 3/4 facility?
- Equipment
- Education
 - First year PHD student
- Other countries will increasingly want to build due to COVID
 - May not have same level of risk tolerance, safety measures
- Level of security is all about risk tolerance to accidental releases
- Most releases are accidental

State Organizations in Bio-Offense/Defense

- Funding constraints = focus

Things that will speed up synthetic biology

- "Cell Free" Technology
- AI & ML to map and sort
- "Gene Fragment Synthesis"

Future Technology

- Technology that allows engineering to control and target bioweapons
- Better testing to determine what works in the field vs the lab
- Screening of viruses to allow engineering

GapsBio-surveillance

- Plant pathogens
- Preons
- Marine micro toxins

LTC Justin De Armond

- Funding models challenge what labs can/can't research - leading to gaps in defense
- Other institutions - CDC in Atlanta; Rocky Mountain Labs
- China has a lot of BSL II labs where security lapses can occur (open bench top work)
 - Higher risk, but all activity / research depends on the risk tolerance of the country/entity
- China is 10 yrs ahead in many aspects
- Nature is currently better than humans in spreading diseases; but with right tech that could be surpassed in the future
- Working to "control" the applications one has created
- Fermi estimate - range of PAX that could be a bad actor with basic knowledge of growing a bioweapon in a tub; risk tolerance
- Print DNA by 2035 - on course to do this with the right tech; \$50K machines that can do this in small batches now

Gaps

- Preons
- Toxins across the spectrum - research abandoned due to international community making use of chemical weapons illegal
 - Maritime - micro toxins
- Biosensors - large gap due to requirement for very sophisticated equipment and the sheer amount of complex soup of biological material to try and track and sense
 - Isomer detection, nucleotide detection, proteins, etc.
 - Samples are messy - lots of stuff to try and sort through
- Plant pathogens
 - Toxins
 - Diseases - virus / bacteria, etc.
 - Easier to starve a population than fire a shot or infect with a virus
- Insect borne diseases

Meeting Notes w/ Dr. Alok Tayi

11 FEB 2022 @ 1300

Participants: Dan Mitchell, Justin De Armond, Tim Harloff, Matt Rasmussen, Laura Porter, Fred Gellert

LTC Justin De Armond:

- Disruptor space is in therapeutics, gene cell therapy, agriculture and climate areas
- Top two take aways
- The microbe / microbial space is an area that needs more research and development
 - Leveraging bacteria
 - Brain / Gut interactions
 - What can bacteria do
 - Researching applications from the simple side of life and engineering that to aid (or harm)
 - Company: Ginkgo-Bioworks
 - Stimulus or changes to the microbes via temperature, pH, other conditions
 - Anti-biotics and resistance - mission critical area
- Domain of Toxicity
 - Buildup of proteins in the body
 - AG impacts for fertilizers, other areas (microbes, virus, bacteria)
 - Airborne / water supply
 - Test similar species or where genes are very close
- Areas of interest
- Capacity / manufacturing capabilities
- Infrastructure shift
- Information / Dis-information
- Pathways and speed
 - How to distribute and incentivize
- Process of development - where can AI assist?
- Crystal graphic structure / database - AI
- Challenge - FDA; #1 rule is do no harm, so slow process in US
- Infrastructure is not flexible
- Goal - make the system Tesla like - copy exactly, speed, remove humans
- Company to look at: United Therapeutics in Taiwan (Covax)
 - Working on vaccines for cow and animals
- China - willingness to do things and experiment; large risk taking
- Company: Culture Bio Sciences: software; bioreactors; fermentation
 - Like Amazon Web Services - access to what you need
- UK - cheMastery; <https://chemastery.com/about-us>; automation, small molecules

- Batch to flow type chemistry / reactions to make processing faster
 - Snapdragon - <https://www.snapdragonchemistry.com/>
- John Cumbers - founder of Synbiobeta; <https://www.builtwithbiology.com/>
 - Biobelt - how to use / repurpose (Google mind)
- Algae spawned all life
 - Need to test ideas and biotech on species that are closely related to humans; find biological similarities and utilize those areas for additional research
- Tons of diseases, but we've let the smaller problems go by and only focus on the large money making ventures; we have knowledge and tech to solve a lot of problems but funding is the major hurdle
- In utero vs. in vitro pregnancy's; when will human life not come from inside a woman; ethical aspects

LTC Matt Rasmussen:

- Machine learning - Process of development – workflow
- Structure relationships
- Identify
- Find correlations in Large groups of data ie protein sequences – predictive analysis of protein chains
- Shift away from chemicals to biological material
 - Infrastructure not sufficient in terms of bio manufacturing
 - Tesla's Gigafactories: The Company's Most Important Innovation? - CleanTechnica
 - Blueprint for bioengineering – flexibility & agility
 - United Therapeutics – Covax – Thailand
 - Testing on animals
 - China – pace, willingness to do things differently
 - Biotech very capital intensive
 - CultureBioSciences – San Francisco – rental bio
- Transition from batch to flow
- SymBioBeta
- Using beer brewing techniques and yeasts – retrofitting coal plants to manufacture bio
- Toxicity – how do you keep chemicals from binding to the proteins you don't want them to, but to bind to what you want it to
- Testing chemicals in multiple types of animals, use machine learning to catalog
- Hubble therapeutics
- Biotech is focused on profits and so only focused on big diseases, not all the small ones
 - Incentives structures not there to answer a large variety of problems in all domains

COL Laura Porter:

- Ph.D., Venture Capitalist, began bench science @ 16y/o. Hx of 16 yrs working with lab automation.
- Agriculture and climate are key areas outside of medical Therapeutic he recommended we focus.
- How do we turn on/off microbiological structures - i.e. environmental, climate, etc. Creation of strains that do not replicate/procreate.
- Antibiotic development/resistance is a mission critical domain
- How microbiological, infrastructure shifts, capacity and capability, Information operations/disinformation operations and pathways/speed of development are key "Biotechnological Threats." How these domains are incentivized and promoted for R&D → therapeutics—>end user is a threat.
- How can AI/Machine learning be integrated in process and development - and where can it be integrated → what step in the process is a key functional area. How can we optimize the supply chain?
- There has been a strategic shift away from Simple to complex entities (i.e. diseases, etc.) due to time intensiveness, resourced dollars. How can machine learning assist with allowing for a transition back to the "simple"?
- Mentioned Google prediction algorithm for crystal structure (CCDC)
- When asked about Dual Use concept w/in scientific community - was not aware of this term associated with malign actors - quantified it w/ a positive construct of "being able to treat multiple diseases"
- Regarding disinformation campaigns - referencing Vaccine misinformation/hesitance and if this is a public opinion, info issue or if fell under the concept of BioTechnology (threat to) - he believes it falls under the guise of a biotechnology threat.
- The agility of Bureaucracy/Agility of Infrastructure
 - FDA has a "do no harm" foundation so drives decisions
 - Economics - how expensive for testing - where does the funding go affects manufacturing. Animal therapeutics has a much lower bar economically - - Easier to manufacture vaccinations, therapeutics - - less bureaucratic (less risk) → how can this be translated to human use/pathways
 - United Therapeutics (based in Taiwan)
 - China has a high pace of development and manufacture - largely due to their willingness to do things "differently" - and their "philosophy"
 - Agile infrastructure - being able to adapt to increased demand for manufacturing needs
 - Tesla Model - Decrease need for human intervention; software scripting; speed; standardization
- Automation - Cultured biosciences - low cost infrastructure. Companies in place with necessary infrastructure capabilities - client "rents" their system/processes for production. Company name "Chem-mastery" is a low cost entity doing this.

- Snapdragon Chemistry is a company working with the Transition from Bach to flow which he indicated is another opportunity. [LOW COST - LOW INFRA-STRUCTURE]
- 3D printing "Jennifer Lewis" doing research in this area [LOW COST - LOW INFRASTRUCTURE]
- Biofermentation company GinkoBioworks [LOW COST - LOW INFRASTRUC-TURE]
- Synthetic Biology - Synbiobeta → company name
- Simulation capability - significant especially in the manufacturing realm
- Domains of Toxicity - being able to test with better modeling (human vs. ani-mal w/ similar genomic patterns) → then using AI to quantify risk for approval purposes - - vs. having to do potentially unrelated animal modeling to pass the bureaucratic hurdles to get into human testing.
- What scares him - - Not having therapeutics for common diseases d/t funding and efforts going to more novel or economically lucrative diseases/pathogens, etc.
- SciFi → transitioning from in utero to invitro gestational capability.

Meeting Notes with Dr. Robert Norton

9 March 2022 @ 1100 via Teams

Attendees: Justin De Armond, Tim Harloff, Matt Rasmussen, Laura Porter

LTC Justin De Armond:

- Prior mil / infectious disease for 35 years
- Problem – things of past will be things of the future
- Biopreporat – huge system
 - Today – nothing is being done at a large scale
 - Smaller and more lethal
- BLS3/4 facilities – big surge in those facilities
- Auburn U – waiting in que for a new facility (only so many companies that build them)
- Track companies that are building the BSL facilities – track where the \$
- How do you locate something with a small signature
- How to discern what is in academia across the world? How do you do that?
 - China
 - India
 - Russia
 - Dual use at worst – weapons programs
 - Rat lines that enable programs to be dispersed worldwide that are integral to their programs
 - Programs are divided up
- Virus can be diverted from medical systems
 - Smallpox that admit it – US / RUS
 - Others likely have it
- Greatest biological weapons are natural diseases
 - Deliver at the speed of travel
- COVID lessons learned – take a look at this
- Testing of wildlife for viruses / disease to see what changes? My thoughts
 - Skip humans and let it replicate in animals and then it transitions to humans
 - Cows, Pigs, Chickens – biggest targets
 - Birds, Bats – move constantly
- Biowarfare in UKE – NATO might have to respond
- Nanoparticles are an issue
- mRNA is an issue for DNA – changing things in hypatic cells (liver)
- Vaccine could be an effective biological weapon
- China, Russia hiding things, but discoverable
 - Technical analysis from missiles helps
 - Issue – bandwidth on how to do this
 - Trackable – resources, and what doesn't get done to do this
 - Reports to Retired General Burgess
 - Big gaps

- "We really don't know?" but we should be able to know
- Cyber is useful to track actions
 - Digital exhaust – we have lots of info around Wuhan; all trackable
 - Help ID facilities
 - Resume intelligence – facilitated by tracking academics who are working X projects
 - Multi-databases (China) CNKI – easy to track; wonfang
 - Repository for all research in China
- Track decision groups
 - Look at funding lines at the bottom of their articles
 - Code means something; which programs are funding that research
 - OPSEC error made by China – can't change what they've done
- Genetic specific changes / virus
 - Target genetic populations
 - Exploit certain genes
 - Preons – coated by genetic material; protein
- Zoonotic diseases– future issues – Foot Stomp!
 - Over 200 that we know of....
- Humanitarian Crisis – Putin
 - How do you stop PAX coming towards you and they've been weaponized
- Detector capabilities – important interest to Auburn
 - Dogs – vaporwake (patented breeding process)
 - Detect disease / pathogens
 - 1/trillion level
 - Detecting viral particles
 - Can pick up metabolic changes from a distance
 - Wasps – detector colony
 - Possibly lower than 1/trillion
 - Combo of dogs/wasps – what other animals are capable of this?
 - Nothing electronically capable to measure it
- 2035 – dogs can detect disease
 - Interface between the dog and electronics
 - Doug the dog from UP (Nuralink – Musk)
 - Biochemical and translated to an electronic signal and then received by our systems
 - Can be trained to detect electronics
 - More than smell – ALL of their senses; an aura around the dog
- Measures and Signals Intelligence (MASINT) – multi-spectrum observation
 - What changes at the metabolic process changes; rapid
 - Airframes, drones, etc.
- 2035 sensors in cities detecting all of these things; size of a phone or smaller
- Public health is not an intelligence process
 - ProMED system? – intelligence the process
 - Vetted, but not as much as it should be

- Authorities that help or hinder this transition?
 - Improvement in communication / transparency / lines of trust
 - How to implement – Lines of Commo; improve
- Future events – operational process and what individuals, groups do in the system
- J2 process – medical needs to impart over the horizon issues; Soldiers are down due to disease and can't pull triggers anymore

COL Laura Porter

Dr. Norton, Ph.D. is a professor at Auburn University in the Food & Water Defense Working Group, Retired Army LTC. 34 years of experience in Infectious Disease

Dr. Robert A. Norton, PhD, is a professor at Auburn University and currently serves as coordinator of National Security Initiatives in the Auburn University Open Source Intelligence Laboratory and program director of the Futures Laboratory, a collaborative effort between Auburn University, Auburn University at Montgomery and Air University at Maxwell Air Force Base. A long-time consultant to multiple federal agencies and the Department of Defense, Dr. Norton's research interests include public health/one health, intelligence analysis, chemical and biological weapons defense, medical and technical intelligence, military-related science and technology, biosecurity/biodefense, and veterinary infectious diseases.

- The federal government tends to look at the past.
- Referenced historical use of "Biopreparat" commenting it was a huge system with large signature - not applicable for today
- Need to think **small scale** equating to lethality. Showed a 5" X5" box and indicated it is easily hidden in medical/academic/military environments, not easily detected and has the capability of high lethality depending on what agent it contained.
- Can Track who is making BSL-3-4 labs (who are the contractors?). Auburn is awaiting the ability to build one.
- What is in the academic world needs to be tracked for Dual-Use capability.
 - Research can be conducted over multiple countries and hidden
- Access to organisms/pathogens can be relatively easy. Many can come directly from the environment (C. Botulinum spores, Antrax, E. Coli, etc.).
- Viruses can be diverted from medical systems. Example - US & Russia have smallpox which was obtained from a viral specimen.
- Spores are easier to build/develop → viruses are the hardest
- Do not have to have biotech to manipulate organisms i.e natural diseases which are naturally/selectively modified based on extrinsic factors
- Look at lessons learned from Covid-19
- Delivery Systems - can be utilized well below the threshold of war.

- Allows for plausible deniability
- A Vaccine can be an effective bioweapon if it can change genetics
- China is hiding things but they are discoverable
 - Digital Exhaust (electronic signatures from personal devices, etc.)
 - Resume intelligence - track resumes from academics working on projects
 - CNKI & Wongfang Databases - Chinese repositories for all academic research within China and is searchable.
 - Bottom of all Chinese academic papers has a code at the bottom and is identified with the program who developed it - utilized as a funding identification. → Is an OPSEC failure on China's part
- Future issues -
 - Genetic specific pathogens - targeting genetic populations to make genes more exploitable (Referenced the new James Bond Movie).
 - Prions
 - Diseases/genetic predisposition - i.e. Sickle Cell trait/Dz. It is a beneficial mutation in some locations - but could be exploited
- Zoonotic diseases are the largest issues
 - Good source material to create bioweapons
 - Impacts food source - naturally occurring death of herd/flocks - culling.
 - Impact of companion animals - (psychological impact/fear)
- Creation of humanitarian crisis
 - Taxing the medical/political/societal systems to address the crisis in and of itself
 - Crossroads of a humanitarian migration/crisis with military operations (referenced 101st w/ Ebola)
- Stressed multiple times - - small scale - this does not take a lot, and does not require any 'tech' at all. Showed an example of a 1.8ml vial with very small amount of white powder in it as an anthrax example - said that much dispersed in a shopping mall could "kill everyone"
- Sensor Capability -
 - Detector Dogs (Vapor Wake dogs) (Currently possible at basic levels)
 - Can detect minor metabolic changes, and detect disease and pathogens
 - Can detect at 1pp Trillion (lower than what is currently available electronically)
 - Utilize smell, visual (aura's), etc.
 - Risk - dogs are susceptible to the diseases they are attempting to detect
 - Detector Wasps (nonstinging)
 - Detect at <1pp Trillion
 - Create lines of detection -
 - Dog / electronic convergence (Doug the dog in the movie Up) - electronic sensors in the dogs brain which transmit to a device to indicate what they are detecting.

- Measure & Signals Intelligence (MSINT)
 - Can put sensors in chicken houses, fly drones, planes, airframe, etc. which can detect metabolic changes quickly.
 - Stressed convergence of Bio and Cyber for future capability
- Additional thoughts/opportunities
 - Stressed importance of public health needing to be integral and integrated in the intelligence process
 - CIV-MIL public health partnerships for information gathering and sharing. Info is currently silo'd and reactive in nature
 - What title authorities are impediments to that and how do we deconflict
 - Medical intelligence needs to be more functional and imbedded and prioritized within the Intel communities (i.e. DIA, and J2)
 - Need to think in terms of effects, not necessarily on the agent. Covid as a disease while lethal, the bigger impact was the operational impact, misinformation, fear, etc.
 - Systems break down because of lack or poor medical intelligence
 - Stressed Zoonotic diseases as an ongoing and future area of concern

Email Communication with Mr. Nimalan Paul, Roche Pharma, Bengaluru, Karnataka, India

Re: Hello from Nimalan
Nimalan DJ <nimalan.dj@gmail.com>
Mon 2/28/2022 2:31 PM
To: Porter, Laura COL <laura.porter.mil@armywarcollege.edu>

Hi Laura

Apologies for the delay in getting back to you.

To be honest BSL 3/4 labs are something I have not had the opportunity to track as they are not related to the work I do. However I have read about the Government's push to become self-reliant for vaccines and the like. I also did read about the mobile BSL-3 lab announced by the Govt some time back and that is as much as I know about this space.

For your second question I can throw some light because I was with GE Healthcare till very recently and in product development. Yes it is possible to hack medical equipment but it is not very common in India.

As a global medical device manufacturer we have to ensure we follow all cyber security regulations laid down by various regulatory bodies plus our own "house rules" which means every release we put out into the market cannot get past product delivery milestones if found lacking in cyber security.

Having said that we have no way to enforce this in the hospital environment and even lesser control over home environments which leaves us open to what are known as man in the middle attacks". In the Indian context not much patient information is available online or on a hospital IT system (most of it is paper based and manual) and also there is not much regulation around patient data (no exorbitant fines if a medical report went to someone else). So if an attacker decides to attack a hospital to hold the patient information to ransom there is not much he / she can get out of it. I have known med devices running for years with the standard "password" as the admin password which everyone in the department and the service vendor would know and nothing really happened.

This could change though because we now have a lot of AI based algorithms that reside on the cloud so the incentive / payoff for attackers could increase. Not sure how much of this helped but if there are any follow on questions you may have do feel free to shoot me an email.

Sincerely
Nimalan

On Sat, 26 Feb, 2022, 02:41 Porter, Laura COL,
<laura.porter.mil@armywarcollege.edu> wrote:

Nimalan

Thank you so much for getting back to me.

I am finding the market research for biotech indicates the industry in India suffered an expected downturn in 2020-2021, but the Economic Ministry and other forecasters are anticipating a rapid recovery post covid in the area of research/manufacturing, especially in Therapeutics & Vaccines. With this, the need for BSL 3-4 labs is increasing to accommodate. Are you seeing that upward market trajectory? I am unable to obtain clear data supporting the exact number & location of BSL 3 & 4 labs. Some sources indicate 6 BSL-3, and 3 or 4 BSL-4 labs. I am also now seeing reports of a BSL-3 Mobile lab. Are you able to quantify or provide a source regarding numbers and locations (Human and Animal facilities)? What other Biotech trends are you seeing in the region that are surprising or new to you?

The other major question I have is related to medical devices and equipment. I'm a Cardiac Nurse Practitioner by profession and have experience with pacemakers, ICD's, etc. Knowing the majority of these devices, along with hospital-specific equipment (i.e. programmers, balloon pumps, vents, IV pumps, hemodynamic monitoring systems, etc.) require wireless &/or hardware network capability. Patient home devices are likely connected to medical providers/vendors via unsecured networks. While hospital equipment will network with vendors/Biomed for upgrades and servicing likely through secure platforms. What is the security infrastructure surrounding this? How easy would it be for a malicious actor to hack into the systems and cause all of the Brand XX ICD's utilizing an IP address for the transmission of data from Omaha, Nebraska to be reprogrammed to fire, turn off, etc.? How difficult would it be to introduce malware to IV pumps within a hospital to make them malfunction? Etc.? Have there been any instances of this occurring? In the US there are growing reports of Hospitals being hacked by cyber-criminals and having health information systems held for ransom. Could the same be done for individual patient implanted devices/hospital equipment?

I know this is a lot, and if it is easier to discuss with you via Teams/Zoom/etc. I am happy to set up a time convenient for you. I appreciate your willingness to help me.

All the best,

Laura

Laura L Porter

USAWC AY2022

Seminar 4

laura.porter.mil@armywarcollege.edu

919-906-9933

From: Nimalan DJ <nimalan.dj@gmail.com>

Sent: Friday, February 25, 2022 3:22 PM

To: Porter, Laura COL <laura.porter.mil@armywarcollege.edu>

Subject: Hello from Nimalan

Hi Laura.

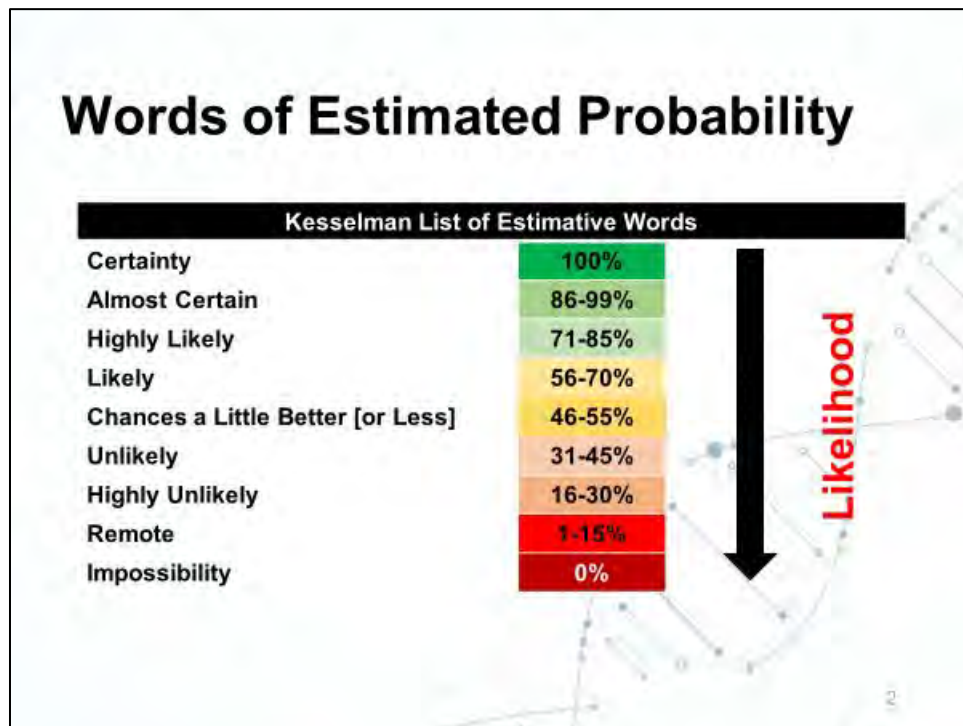
Nice to meet you and glad to share what little I know.

My experience is in med tech (devices) and molecular oncology. Is there any specific area you are interested in?

Sincerely

Nimalan

Annex F – Briefing Slides



Analytic Confidence

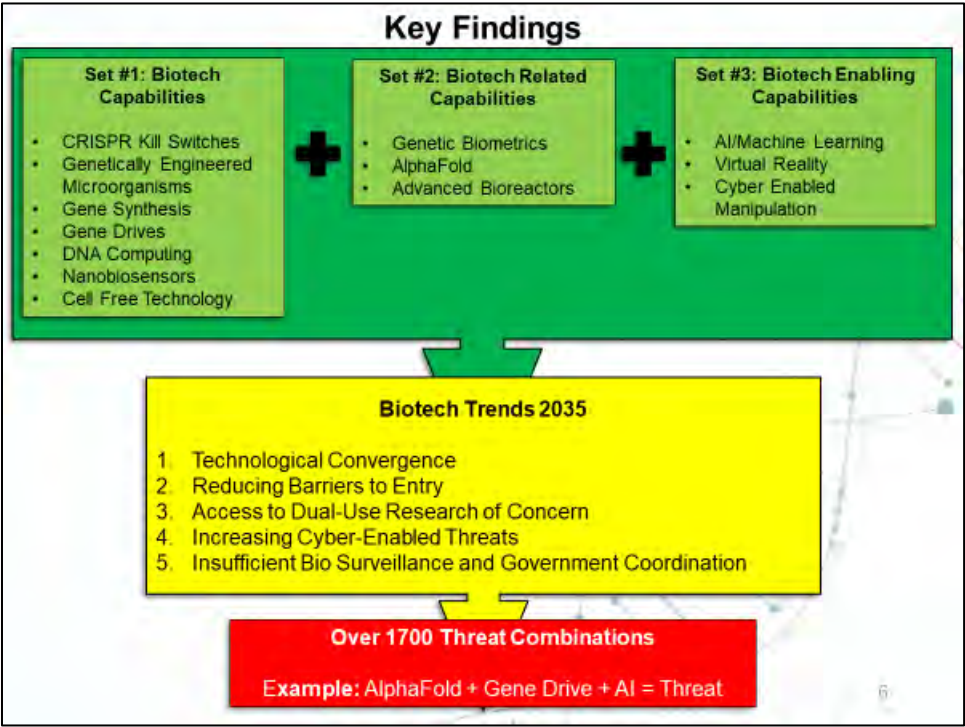
Our overall estimate is ***moderate***.

3

Question

- What surprising biotech capabilities will potentially threaten U.S. people, infrastructure, and/or the military by 2035?
- Sub-questions:
 - What are the most likely U.S. resources (people, infrastructure, organization, etc.) a group would likely target with a biologically based technology?
 - What areas of biotech are adversaries developing threats?
 - What current or emerging technology could be used to engineer or deliver a bioterror with limited resources?
 - Are the developing biotech capabilities reproducible at a small scale, with commercially available resources?
 - What biological processes are being used/developed that could be weaponized by 2035?

| | | Estimative Probabilities of 13 Biotech Capabilities | | | |
|--|----------|--|--|---|---|
| | | Almost Certain (86-99%) | Highly Likely (71-85%) | Likely (56-70%) | Chances a Little Better (46-55%) |
| C a p a b i l i t y S e t s | Biotech | | <ul style="list-style-type: none">- Gene Synthesis- Cell Free Tech | <ul style="list-style-type: none">- CRISPR Kill Switches- GEMs- Gene Drive- DNA Computing- Nanobiosensors | |
| | Related | <ul style="list-style-type: none">- Genetic Biometrics | | <ul style="list-style-type: none">- AlphaFold- Advanced Bioreactors | |
| | Enabling | | <ul style="list-style-type: none">- Virtual Reality- Cyber Enabled Manipulation- AI/ML | | |




The top half of the image shows a stylized illustration of a human brain with various electronic components and wires connected to it, set against a background of floating letters. The bottom half of the image contains text and a faint DNA helix graphic.

**Trend #1:
Technological
Convergence**

Innovations Disrupting Biotech:

- Artificial Intelligence/Machine Learning (AI/ML)
- Advanced DNA Computer Processing
- Nanobiosensors
- Virtual Reality (VR)

8



Trend #1: Technological Convergence

Tech - AI/ML-Enabled Biotech:

- Tech - AlphaFold:
 - Google's AI DeepMind program
 - Predicted COVID-19 structure
- Tech - CRISPR-Cas9

9

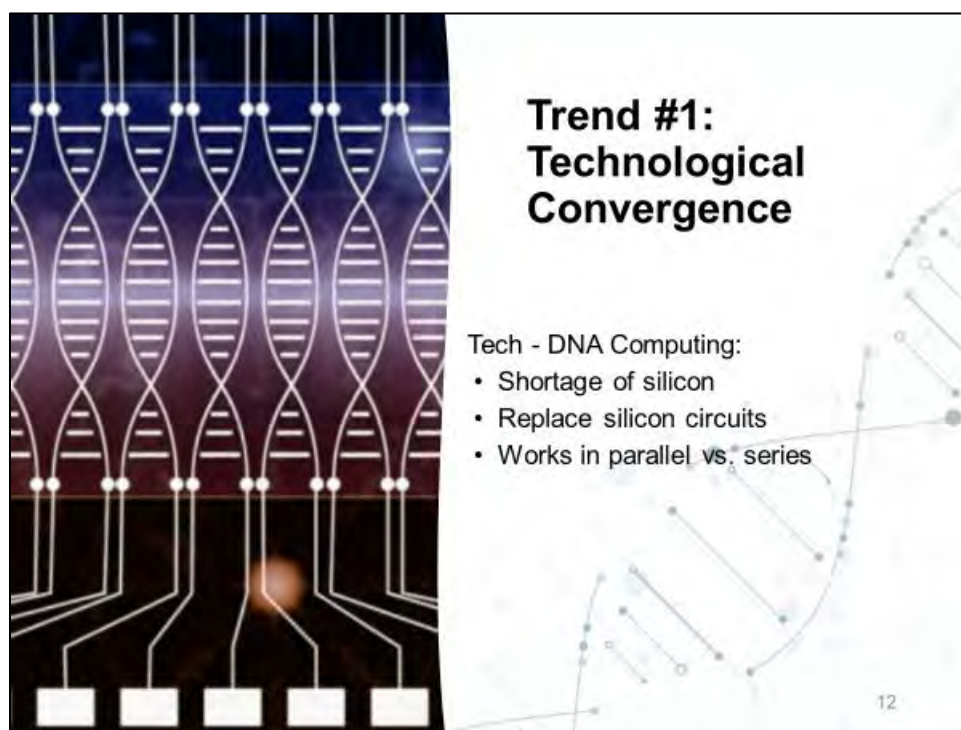
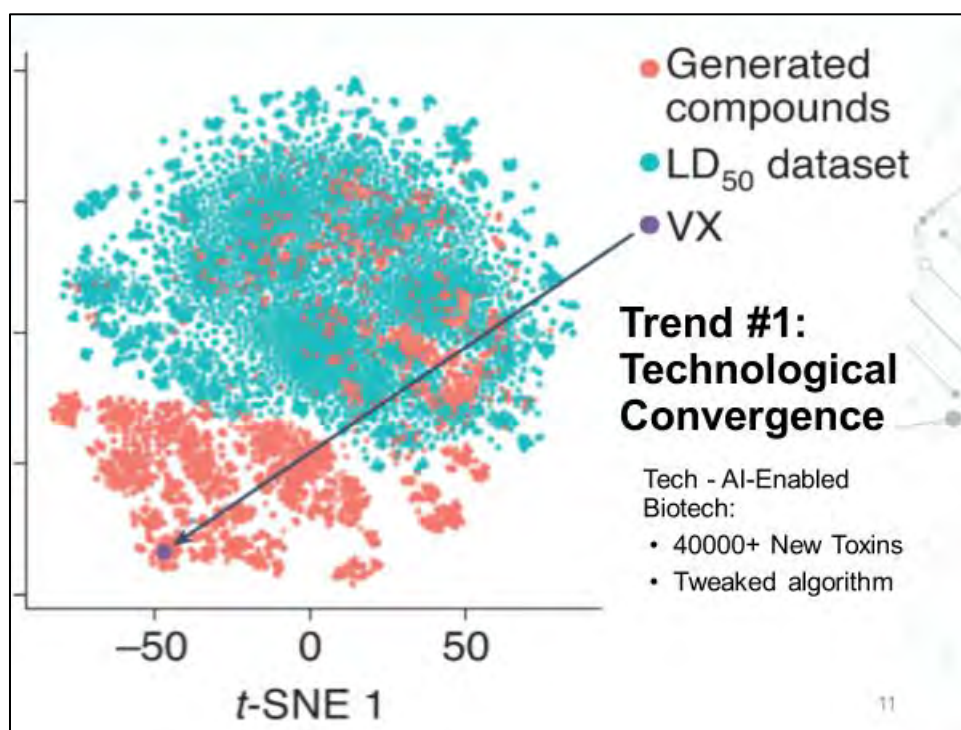


Trend #1: Technological Convergence

Tech - AI/ML-Enabled Biotech:

- Assisting in Food Production
- Satellite Imagery Analysis
- Active & Remote Monitoring
- Predictive Analytics

10



Trend #1: Technological Convergence



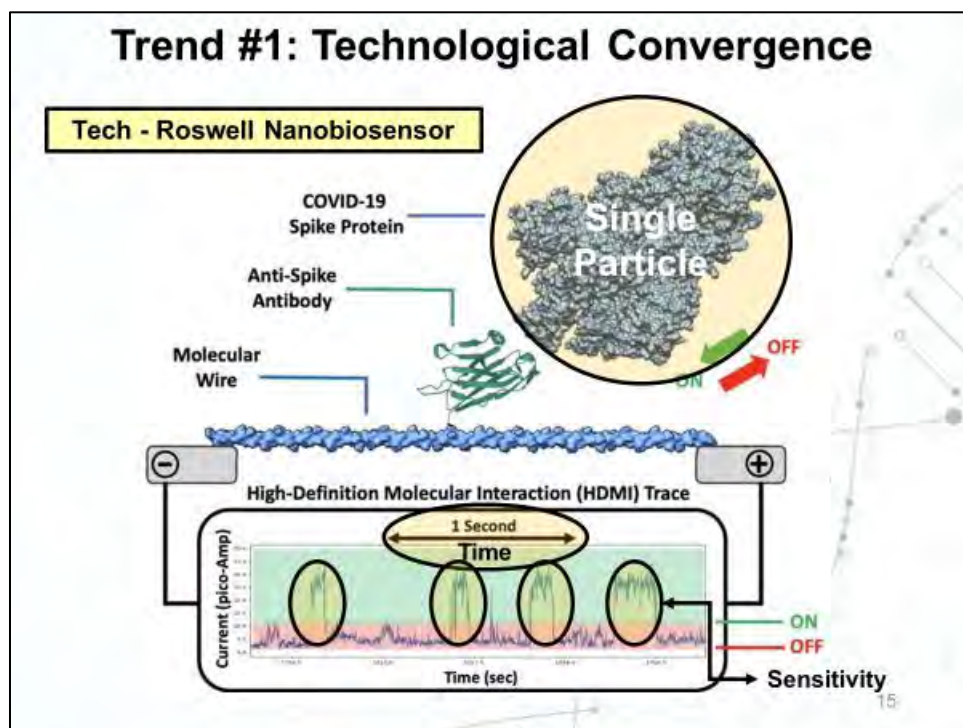
Tech - DNA Computing:

- Origins from 1994
- Total WWW Storage = Cup of Coffee

Trend #1: Technological Convergence

Tech - DNA Computing:

- DNA Nanoengineering
- DNA Origami
- Enzymatic Nicking
- More Efficient



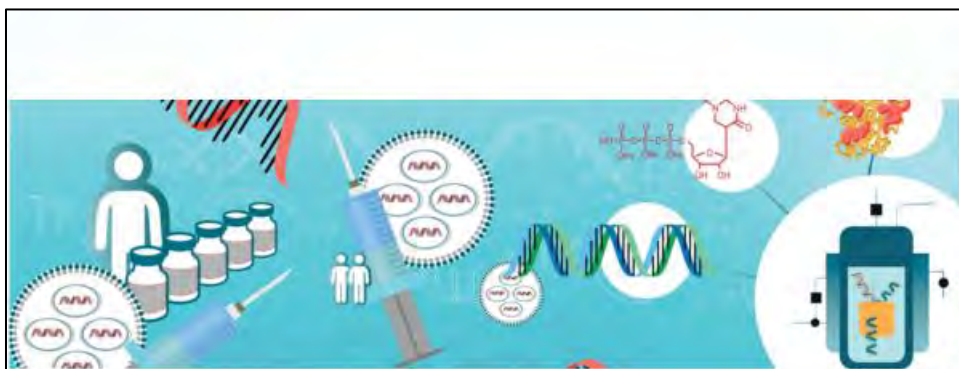


**Trend #1:
Technological
Convergence**

Tech - Virtual Reality:

- Observe inhibitor drug candidates
- Tech - Help develop GEMs

17

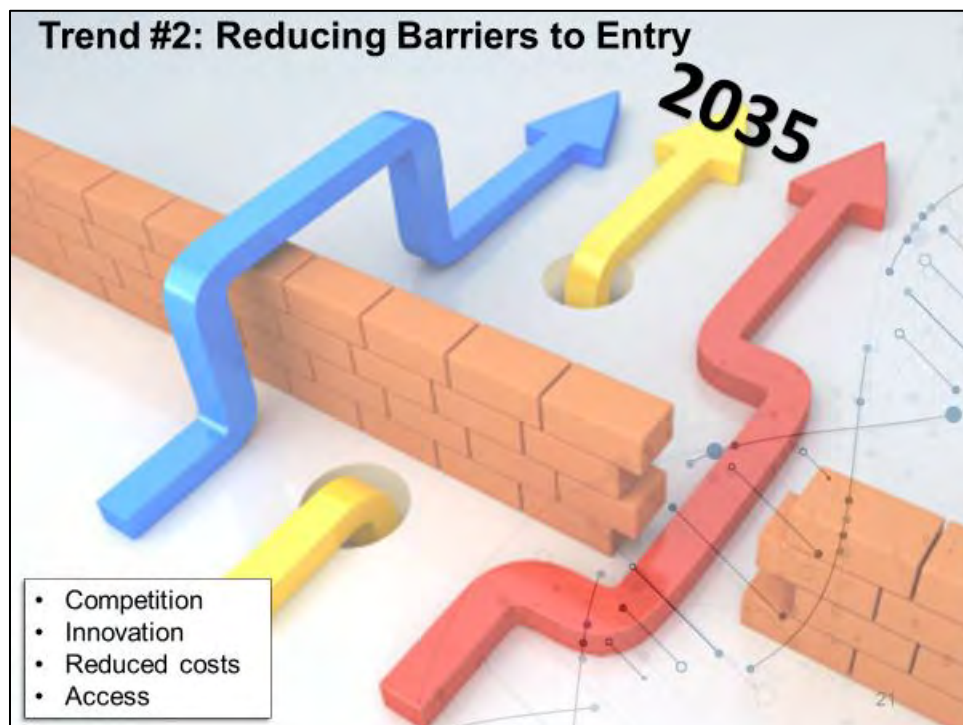


**Trend #1:
Technological
Convergence**

Biotech Automation:

- Tech - Gene Sequencers
- Tech - Gene Synthesizers
- Improved Efficiency
- Better Quality of Research

18





GLOBAL TRENDS 2030

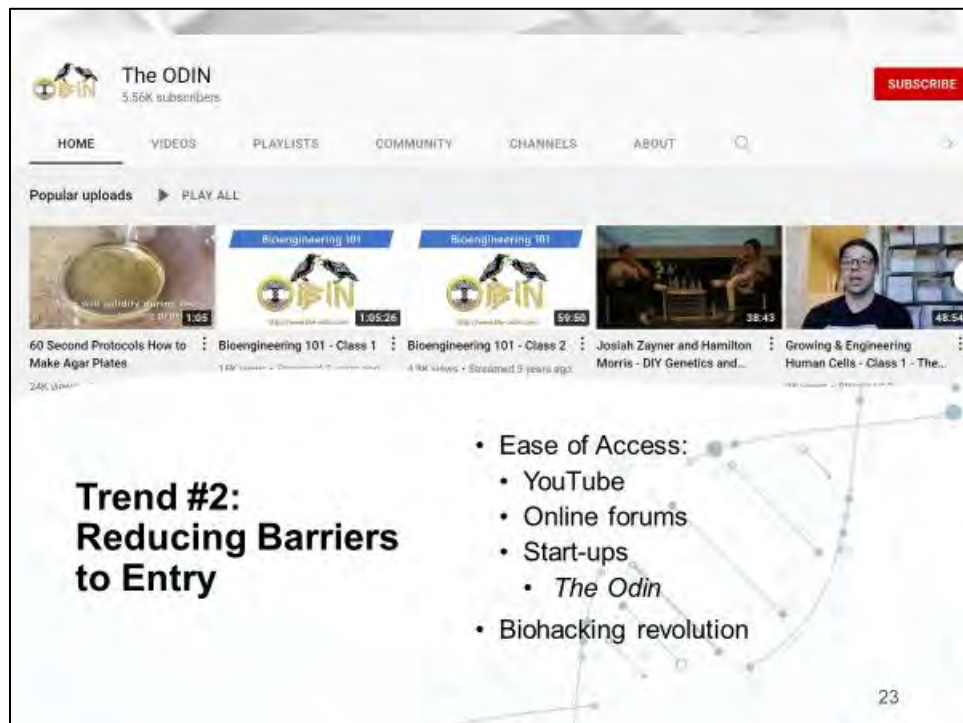
A MORE CONTESTED WORLD

Trend #2: Reducing Barriers to Entry

Biotech Growth:

- Estimated 20% of global economy by 2040
- Main areas:
 - Agriculture
 - Manufacturing

22



The ODIN
5,56k subscribers

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS ABOUT

Popular uploads ▶ PLAY ALL

60 Second Protocols How to Make Agar Plates
1:05

Bioengineering 101 - Class 1
1:05:26

Bioengineering 101 - Class 2
59:50

Josiah Zayner and Hamilton Morris - DIY Genetics and...

Growing & Engineering Human Cells - Class 1 - The...

Trend #2: Reducing Barriers to Entry

Ease of Access:

- YouTube
- Online forums
- Start-ups
 - *The Odin*
- Biohacking revolution

23



Trend #2: Reducing Barriers to Entry



Tech - Gene Sequencers



Tech - Advanced Bioreactors

- Accessible and easy to use equipment
- Not expensive



Tech - Gene Synthesizers

26



Trend #2: Reducing Barriers to Entry

- Easy to obtain organic materials
- DNA databases are open source

27

Trend #2: Reducing Barriers to Entry

- Democratized biotech:
 - No formal training in safety and ethics
 - Potential biohazard accidents
- Lack of Regulations



Trend #2: Reducing Barriers to Entry

- New entry points for learners
- Incorporate genetics education

The Genetic Engineer's Pledge:

"For the betterment of humanity, I pledge, with all my DNA, cells, and knowledge, to never use my genetic engineering mastery, to lay harm on the natural world or anybody."

-Amino Labs





Trend #2: Reducing Barriers to Entry

The top part of the image shows a diagram of the BioBits system. It illustrates the process of adding DNA, RNA, and Protein components to a reaction mixture, resulting in the synthesis of a protein. The bottom part shows a photograph of a multi-well plate containing several wells with different colored liquids (blue, green, red, yellow, orange, pink, purple, light blue), representing different protein synthesis reactions.

BioBits:

- Tech - Cell Free technology
- Protein synthesis without live cells

Enables:

- Ease of use
- Low cost experiments

The number '31' is visible in the bottom right corner.

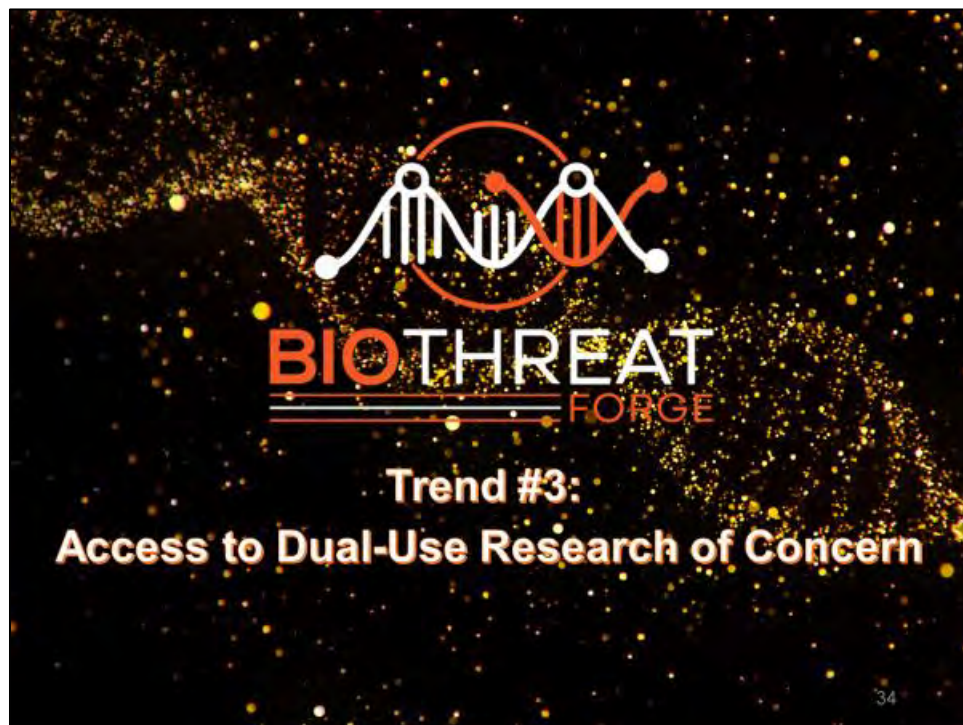
Trend #2: Reducing Barriers to Entry



Threat Groups:


- Nefarious actors
- Non-state
- State
- Hobbyists

32



Trend #3:
Access to Dual-Use Research of Concern

34




Trend #3: Dual-Use Research of Concern

Dual-Use & Ethics:

- Misuse threatens life, the environment, industry, and national security
- China: He Jiankui – edited DNA of embryos
- International rebuke

35

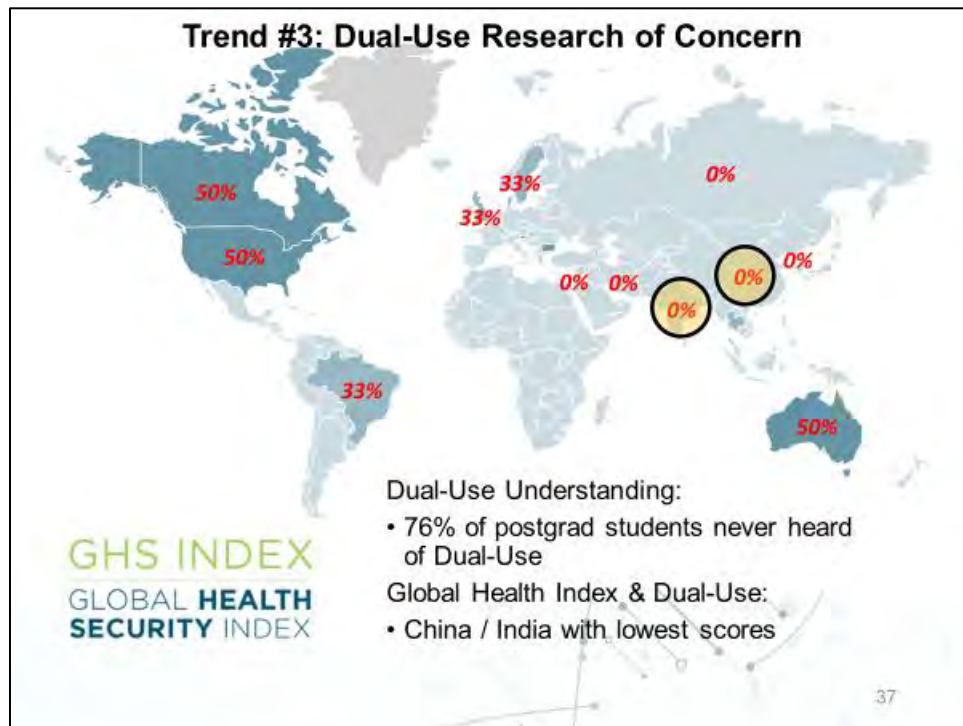


Trend #3: Dual-Use Research of Concern

Military Dual-Use:

- Weaponization
- Scientists mostly see opportunities not threats
- Misunderstand risks

36



Trend #3: Dual-Use Research of Concern

Dual-Use and China:

- Biotech showcased in recent 5-Year plans
- COL Guo Ji-Wei's paper on military use of biotech
- Tech - AlphaFold a tool to assist in reaching goals

Tech - AlphaFold




Trend #3: Dual-Use Research of Concern

China and Gene Editing:

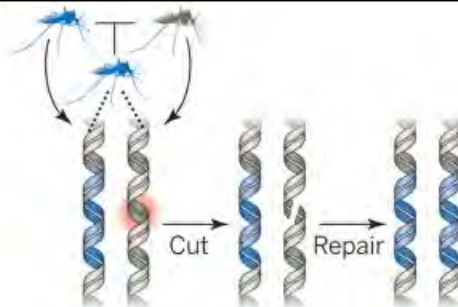
- Biotech as a new military domain
- Tech: Gene Drive



39



Standard altered gene
1 copy inherited from 1 parent
50% chance of passing it on



Altered gene + gene drive
1 copy → 2 copies
100% chance of passing it on

Trend #3: Dual-Use Research of Concern

Tech - Gene Drives – Playing God:

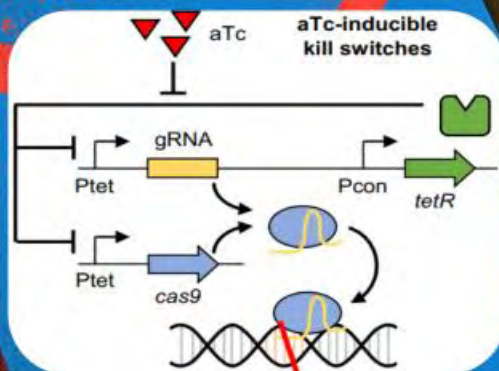
- Preference one trait over another
- Sensitive to specific chemicals or prodrug for activation

40

Trend #3: Dual-Use Research of Concern

Tech - GEM Development:

- Tech - CRISPR Kill Switches
- Programable microorganisms
 - Activate
 - Deactivate
 - Die



41

Trend #3: Dual-Use Research of Concern

Bioeconomy:

- Ethical grey zones
- Genetically Engineered Microbes
 - Tech - CRISPR Kill Switches
 - Potential to kill good bacteria



42

**Trend #3:
Dual-Use
Research of
Concern**

Science is Outpacing:

- Laws
- Policies
- Regulations

International Agreements:

- Insufficient
- Dated

Lacking international
regulatory agency





**BIOTHREAT
FORGE**

**Trend #4:
Increasing Cyber-Enabled Threats**

Trend #4: Increasing Cyber-Enabled Threats

Reliance on a digital backbone



Cyber-Attacks do:

- Steal biological data
- Corrupt physical and digital genomes
- Disturb networks, data storage, and process control
- Disrupt workflows and supply chains

46

Trend #4: Increasing Cyber-Enabled Threats




 **Hybrid CoE**
The European Centre of Excellence for Countering Hybrid Threats

- Manipulated / Corrupt biomedical research data
- Manipulate deep-learning systems

47

Trend #4: Increasing Cyber-Enabled Threats

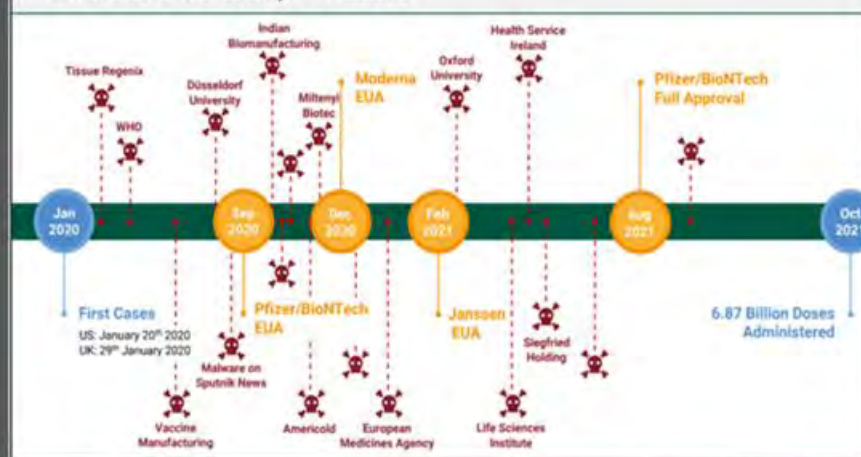


Tech - Hackers penetrate and attack databases

Engineered DNA toxic to recipient

48

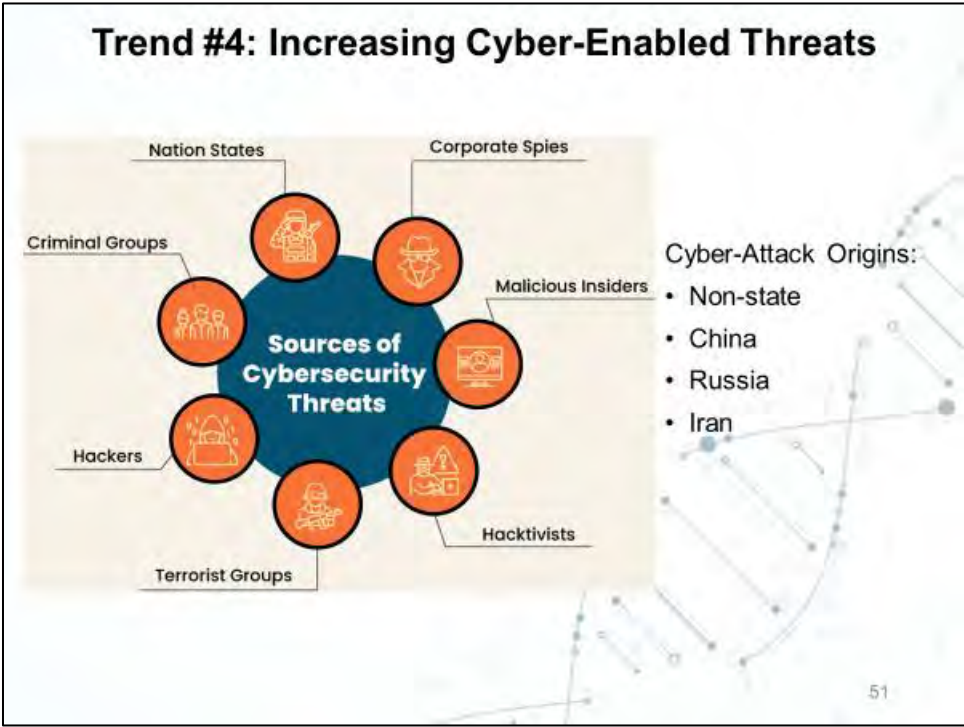
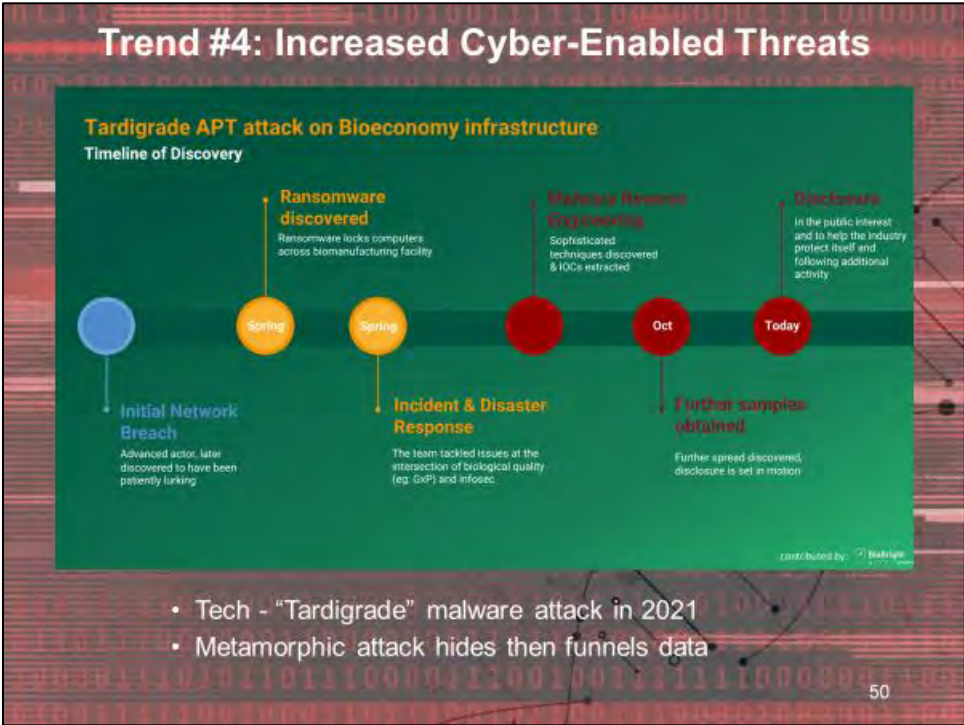
Where are we today? - Attacks



Trend #4: Increasing Cyber-Enabled Threats

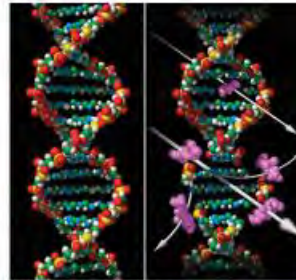
- COVID-19 opportunity to increase cyber-attacks
- More focus on complex targets

49



Trend #4: Increasing Cyber- Enabled Threats

- Cyber-attacks at all-time highs
- Targeting medical industry data
- Delay life saving services
- Target specific individuals



52

Trend #4: Increasing Cyber- Enabled Threats

Tech - Genetic Biometrics:

- Cyber-Hacking almost certain
- Domestic surveillance
- DNA used to ID anyone



53



Trend #4: Increased Cyber-Enabled Threat

Tech - Genetic Biometrics:

- Used to determine genealogical ties
- Potential to target family members

Your DNA Test Could Send a Relative to Jail

54

Trend #4: Increased Cyber-Enabled Threat

Tech - Genetic Data

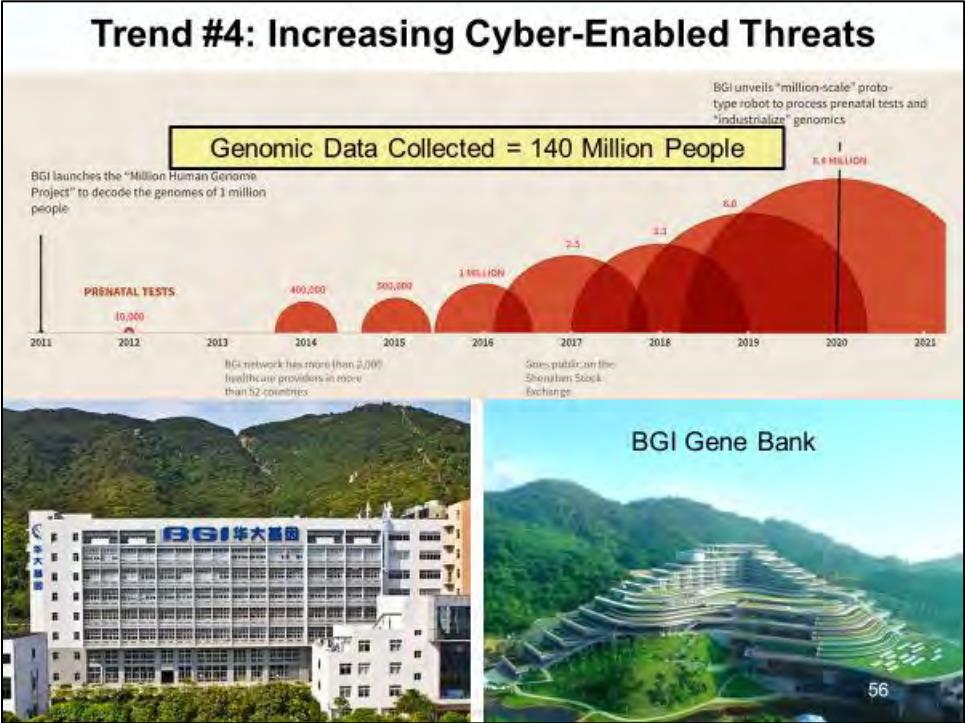
- Chromosomal analysis
- DNA analysis
- RNA analysis

Anthem BlueCrossBlueShield Data Breach

EQUIFAX

AFDIL
Armed Forces DNA Identification Laboratory

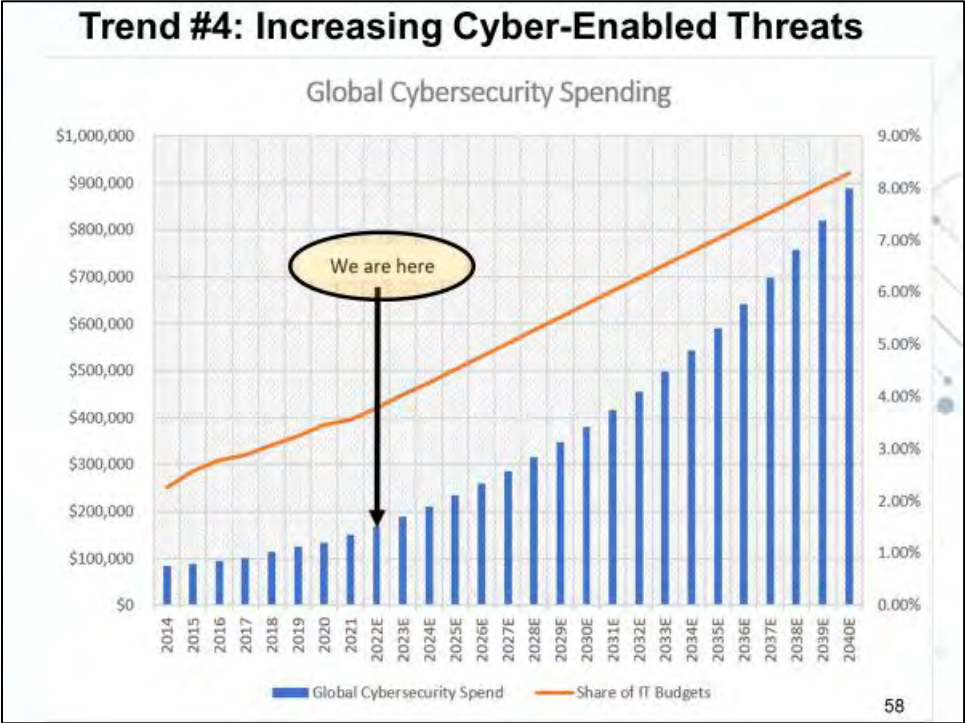
55



Trend #4: Increasing Cyber-Enabled Threats

- Need to protect service member DNA
- Risks of DNA sampling via gene sequencers

57



BIOTHREAT FORGE

Trend #5:
Insufficient Bio Surveillance and Government Coordination

60

Trend #5: Insufficient Bio Surveillance and Government Coordination



- INSS states biot threats as national security concerns
- State and Non-State actors using COVID-19 response against U.S.

61

Trend #5: Insufficient Bio Surveillance and Government Coordination

- Bioterrorists looking to cause widespread damage
- Need rapid detection and response capabilities



62

Trend #5: Insufficient Bio Surveillance and Government Coordination

BioWatch Program:

- Insufficient warning system
- Limited Capabilities
 - Air
 - Water
- Inadequate sensors




63

Trend #5: Insufficient Bio Surveillance and Government Coordination

Tech - Nanobiosensor benefits:

- Fast
- Cheap
- Accurate



 roswell

64

Trend #5: Insufficient Bio Surveillance and Government Coordination

Health Crises:

- Inconsistent focus
- Inconsistent funding

Where cutting public health funding would hurt most

PUBLIC HEALTH FUNDING
A MISSED OPPORTUNITY?

Trend #5: Insufficient Bio Surveillance and Government Coordination

Public Health Initiatives:

- Decreased funding
- Less surveillance measures

Trust Issues:

- Lacking in public health institutions
- Inequality and lack of cooperation

Trend #5: Insufficient Bio Surveillance and Government Coordination

Public Health Failures:

- Non-effective coordination and collaboration
 - State
 - Regional
 - National



67

Trend #5: Insufficient Bio Surveillance and Government Coordination

Bio Surveillance Systems:

- Civilian Agencies are the lead
- Perceived need for better coordination



68



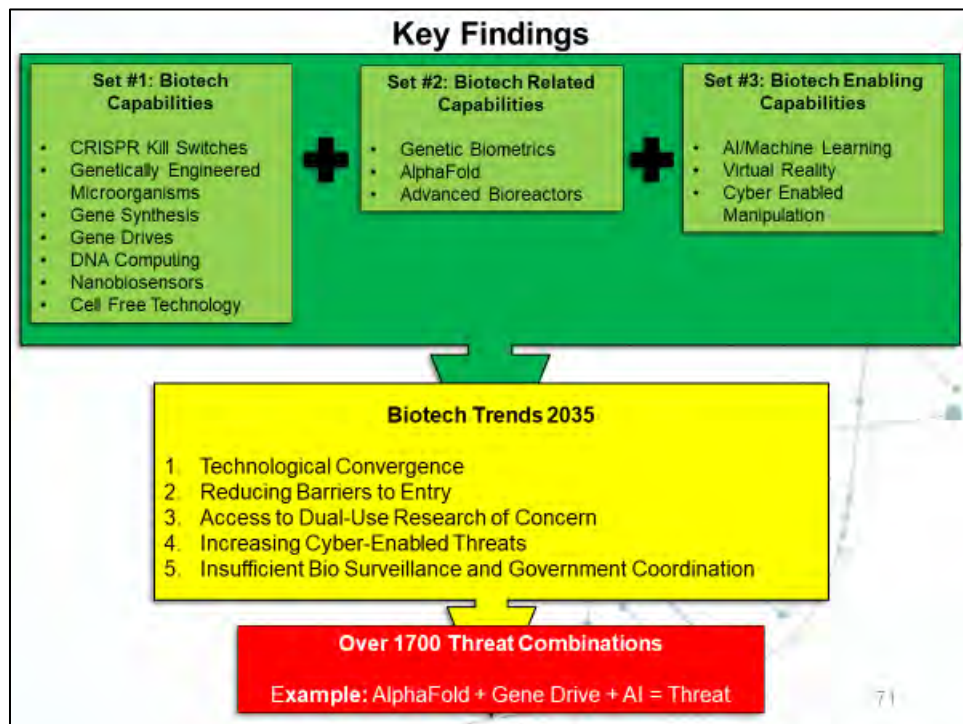
Trend #5: Insufficient Bio Surveillance and Government Coordination

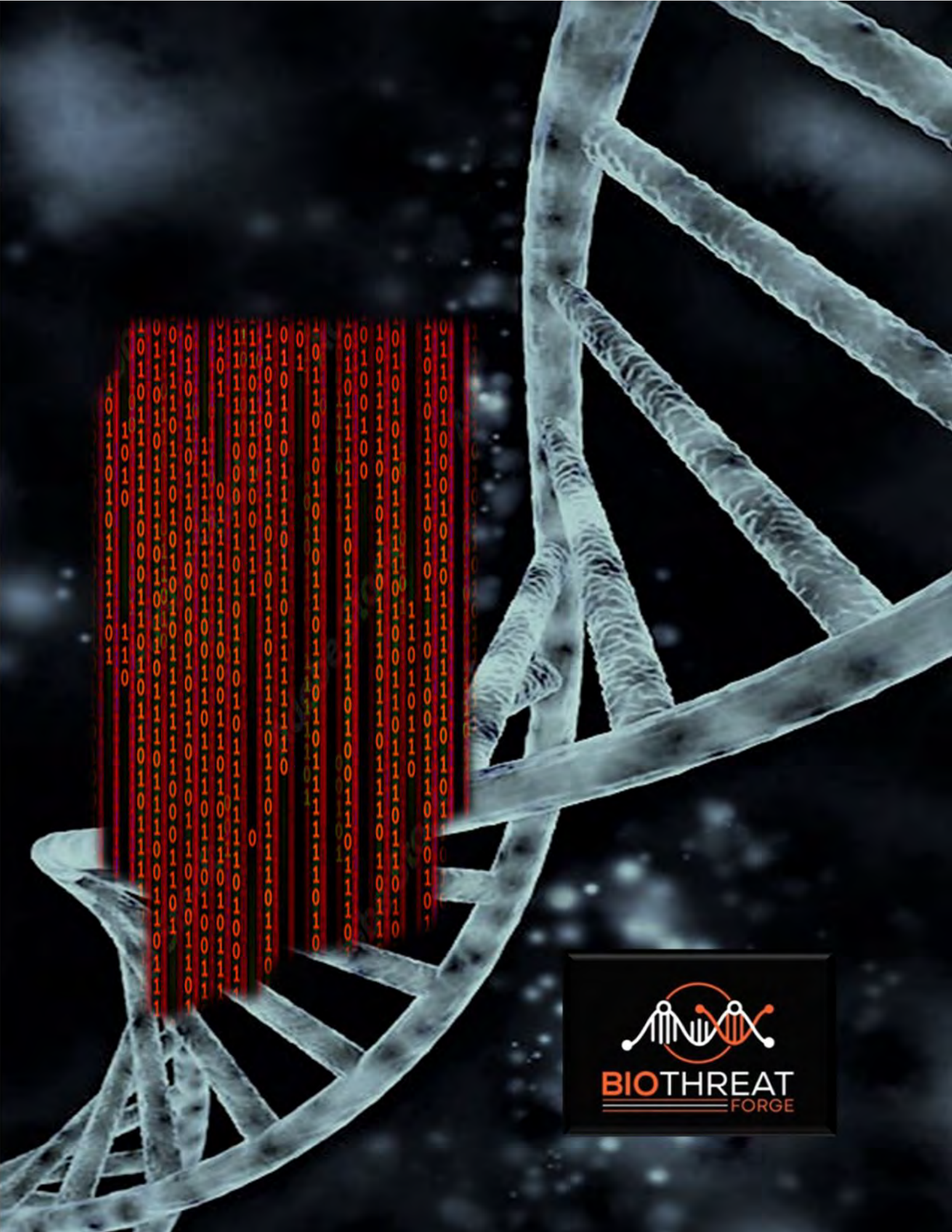
Bio Surveillance Systems:

- Need synchronization
 - Monitoring
 - Analysis
 - Action Plans
- Impact
 - Larger biotech threat



69





BIOTHREAT
FORGE