Security Vulnerabilities in the Bioeconomy Existed Prior to Synthetic Biology

Randall Murch, PhD
Research Lead and Professor of Practice
Virginia Tech – National Capital Region
IPA to the Defense Threat Reduction Agency/Cooperative Threat Reduction
Presentation to the NAS National Materials and Manufacturing Board
May 1, 2019

VIRGINIA TECH

Starting Point

- The convergence of the spectrum of the life sciences and information technologies and infrastructures presents significant opportunities and benefits but also presents significant vulnerabilities, many of which are unrealized
- The realizations and characterizations of these vulnerabilities began several years ago, focused mainly on “Big Data”
- “Big Data” is just one of many “vulnerability spaces”
  - Today the view of vulnerabilities is broadening and gaining greater recognition and clarity through more thorough and rigorous treatments and an organized approach (e.g., “Cyberbiosecurity”)
- Understanding of and solutions to these vulnerabilities require blended teams of experts – it is not just “cyber” applied to “bio”,
  - Deep knowledge of adversaries’ goals, objectives, and technical and operational tactics, techniques and capabilities are also required
- Using system-of- systems approaches and methodologies will produce the most benefit (studies & analyses, outcomes)

Some Emerging Bioeconomy & Biosecurity-Related “Big Security” Challenges

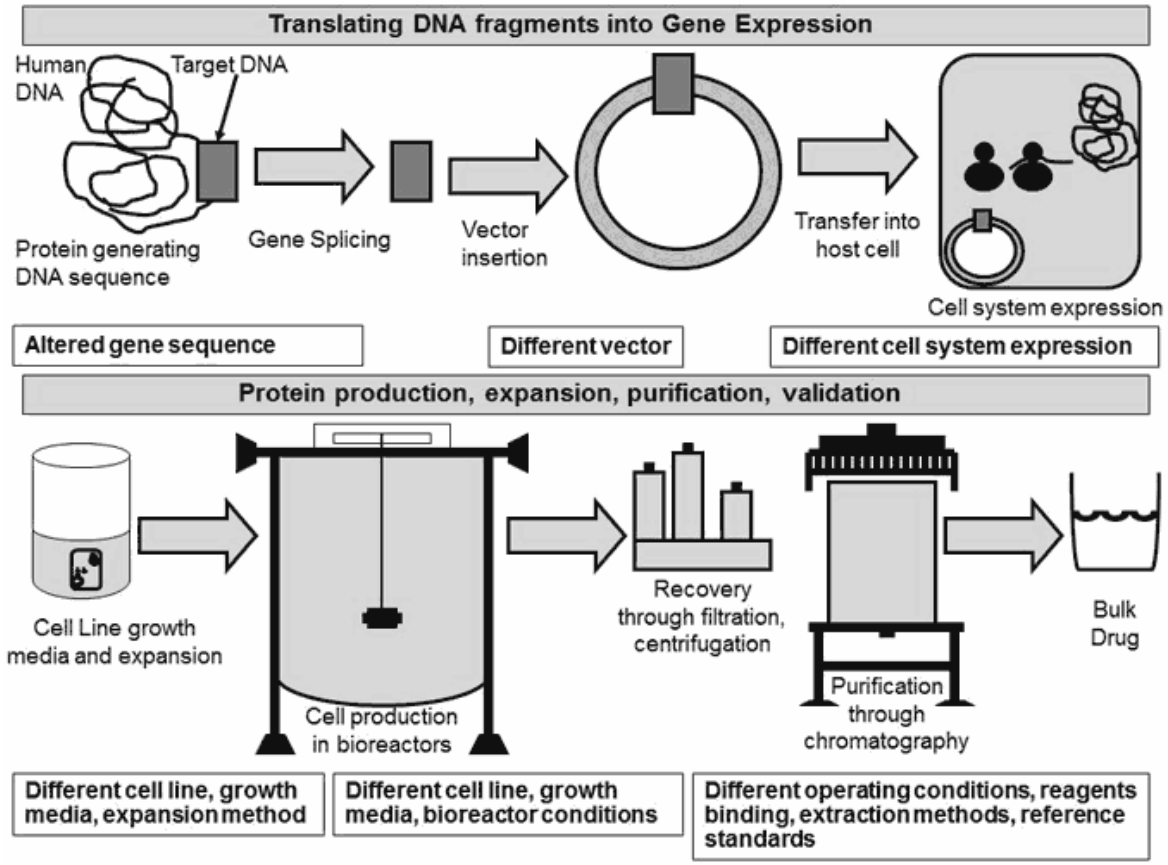
- Security and Integrity of Metadata, Genomics, Bioinformatics, Data Analysis and in (Data/Microbe) Repositories
  - On Site and Transactional Between Sites
  - Protecting and Ensuring the Integrity of Intellectual Property, Sensitive Metadata/Personal Information and Relationships
- Preventing Compromise and Corruption of Bio-Oriented, IT-Dependent Manufacturing, Production and Logistics, Medical and Health Devices and Systems (i.e., Sensors, Monitoring, Medication Delivery, Robotic Surgical Systems)
- Security of Sensitive, Critical Data and Data Sharing (Including “In the Cloud”)
- Preventing the Misappropriation and Misuse of Science for Illicit and Nefarious Purposes in IT-Supported Systems
- Prevention of Disruption of Facility-Supporting Infrastructure
- Prevention of Disruption of the Supply Chain (e.g. Drug Manufacturer to Patient or “Farm to Table”)
- Maintaining Scientific Openness While Ensuring Protection of Scientific and Technological Processes, Outputs and Outcomes

Summary: Systems Analysis of a Biomanufacturing Facility

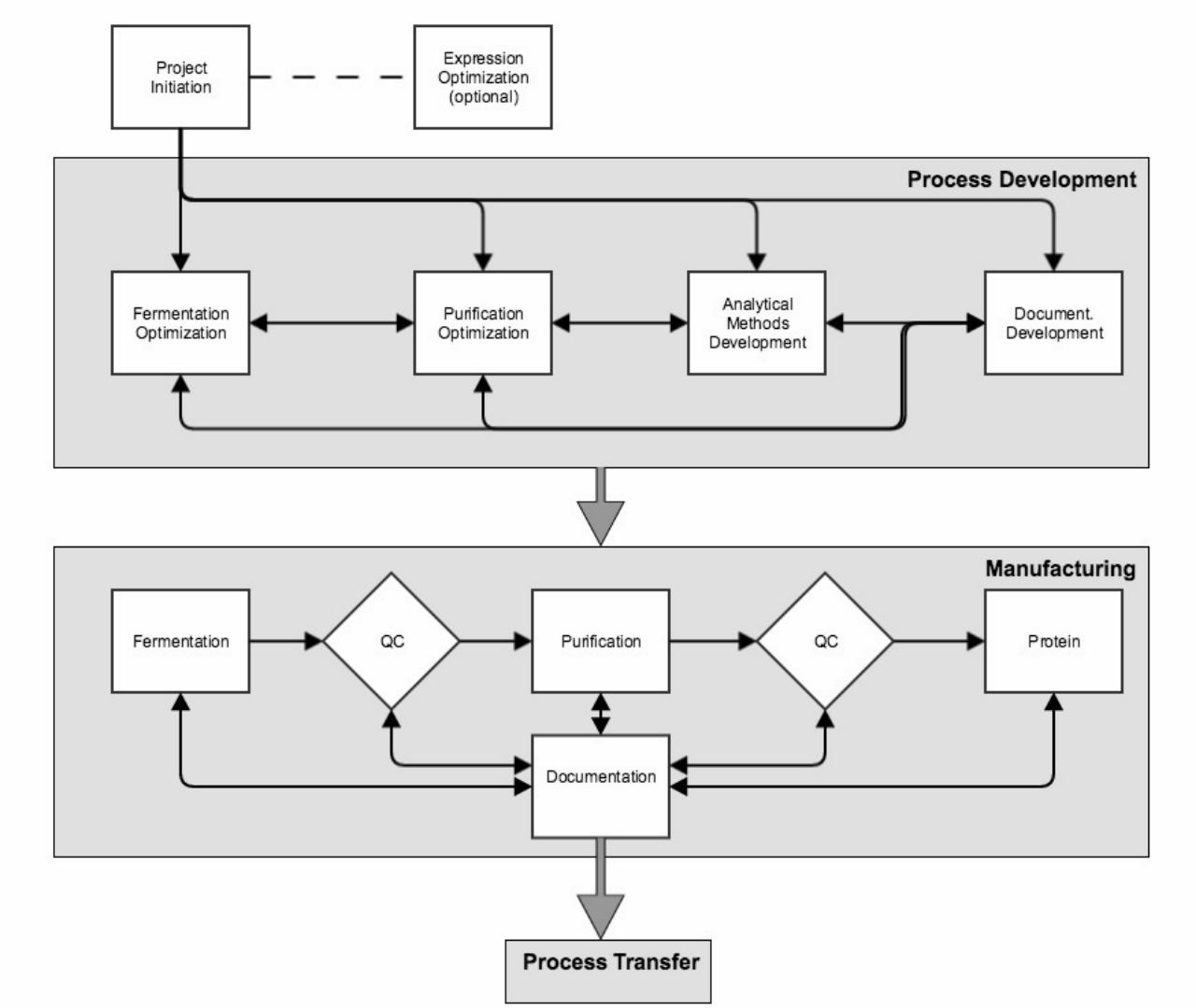
- Period of Performance: Sept 2016 – Sept 2017
- Conduct a System Analysis of the University of Nebraska Biological Process Development Facility (BPDF) from the "Cyberbiosecurity" Perspective as:
  - Task 1: Characterize the Information and Physical Ecosystems of Biomanufacturing (4 months)
    - Baseline Evaluation of the BPDF Ecosystem
    - Focused Analysis of Critical Information and Key Functions and Operations
    - Mapping the Physical Supply Chain Transactions
    - Formulation of the Interim Report and Preparation for Next Steps
  - Task 2: Perform Focused Analysis of Prioritized Vulnerabilities (aka "Deep Dives") (4 months)
    - 4 Overarching
    - 10 Specific
  - Task 3: Generate 3 – 4 Scenarios and Develop a Concept of Operation (CONOP) (3 months)
    - Scenarios: 11 for Use for Subsequent Analyses and Exercises/Gaming
    - Two "Operational Views" (BPDF-Focused and Strategic Campaign-Focused)
    - CONOP: Future Planning
  - Task 4: Final Report (1 month), FOUO (Not Available to the Public)

- Sponsor: Department of Defense
  Stakeholders: Several USG Agencies
- The Project Team and Support
  - Project Team: Virginia Tech, University of Nebraska – Lincoln, Colorado State University
  - Project Support: National Strategic Research Institute (NSRI) at the University of Nebraska
- Project Foci:
  - System-of-Systems Approach, Integrating:
    - Biological Process Development and Scale Up
    - Supply Chain
    - IT Support Systems and Cyber-Physcial Interfaces
    - Facility and Infrastructure Security

Initially, Cyberbiosecurity was Defined and Developed Using a Biomanufacturing Model



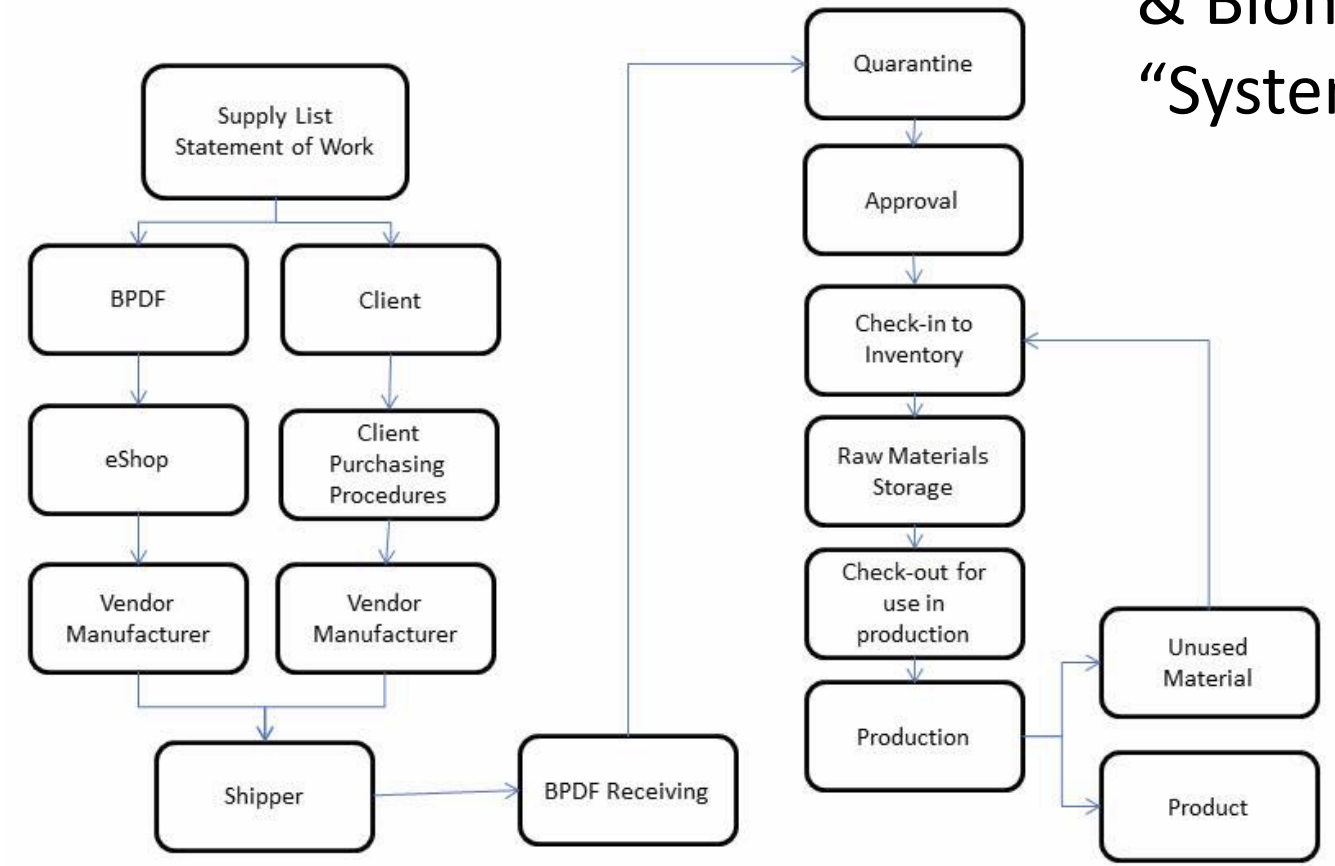
- The development of a proteinbiomanufacturing process starts with genetic engineering operations to develop a cell line capable of expressing the protein of interest in large quantities.
- Large volumes of these cells are grown under defined conditions and the protein is extracted and purified from the resulting biomass or growth medium.



Bioprocess Development & Biomanufacturing: "System of Systems" (1)

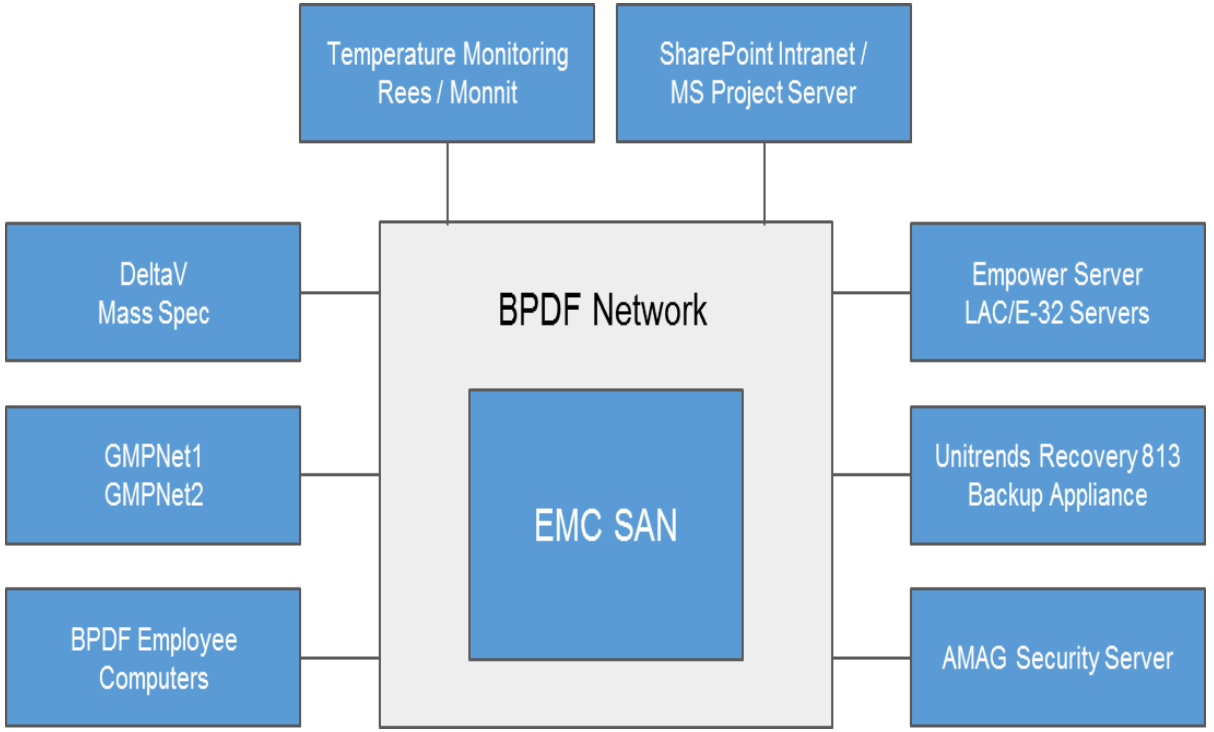
Overview of a Biological Process Development Facility (BPDF) project workflow

Bioprocess Development & Biomanufacturing: "System of Systems" (2)



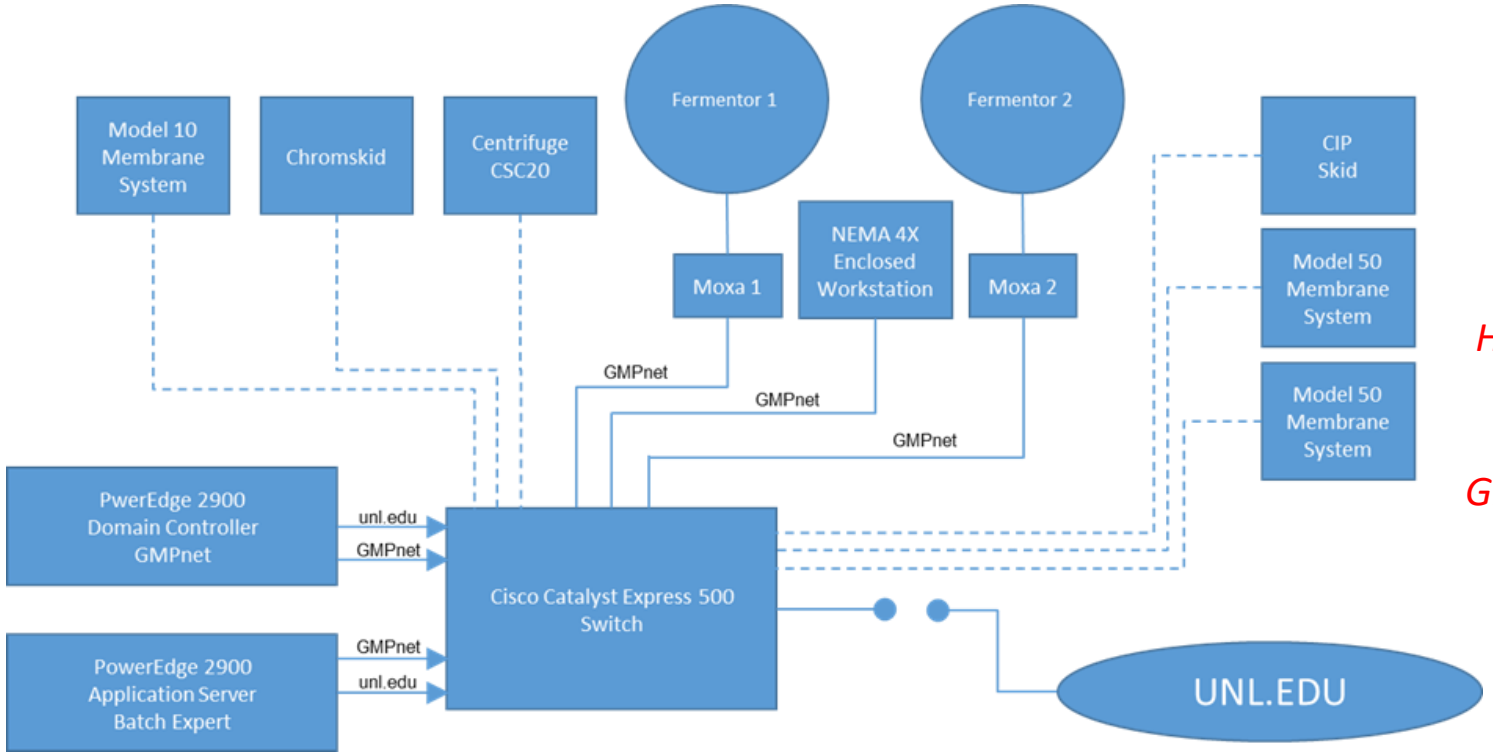
"Supply Chain": Process for acquisition of raw materials and consumables; procurement, receipt, and storage until use.

Bioprocess Development and Biomanufacturing is Supported by an Information System Infrastructure (1)



High-level depiction of a Bioprocess Development Facility (BPDF) Information System Infrastructure

Bioprocess Development and Biomanufacturing is Supported by an Information System Infrastructure (2)

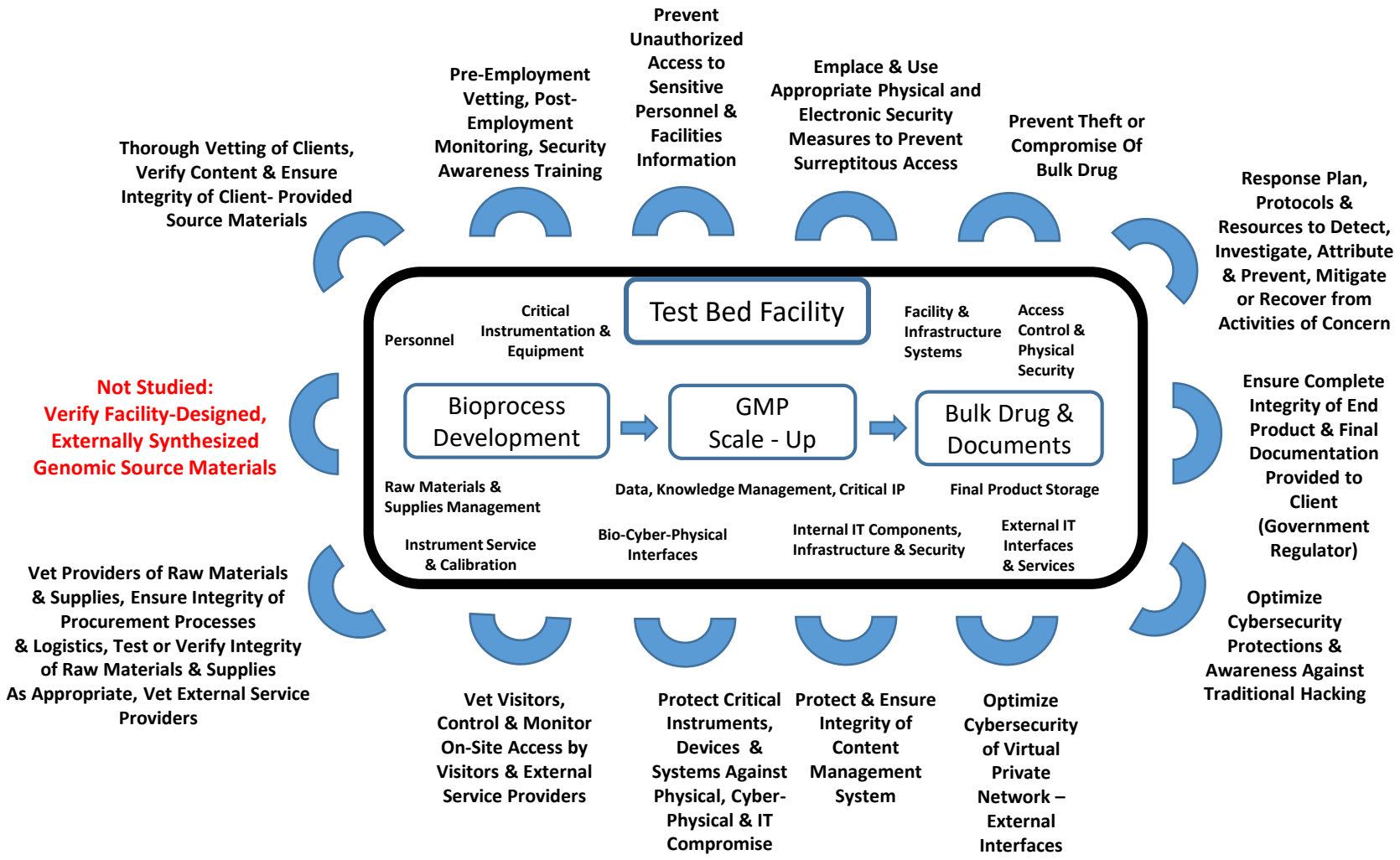


High-level depiction of a Bioprocess Development GMP facility network

Some Vulnerabilities Recognized from the Analysis

- Surreptitious monitoring of activities and information to steal intellectual property or provide “operational intelligence” for subsequent nefarious activities
- Compromise of IT systems that result in corrupted data or communication links for secondary objectives
- Corruption of key aspects of bioprocess development or biomanufacturing resulting in a suboptimal or compromised product
- Induction of failure of key infrastructure components which results in negative impacts to bioprocess development or biomanufacturing
- Alteration of biologic (i.e., genomic, proteomic) data or bioinformatics analysis of such data which is being communicated through IT systems resulting in unwanted or harmful outcomes or downstream effects
- Negative interventions in the Supply Chain which result in contaminated reagents and consumables, could be aided by surreptitious cyber monitoring of communications or transactions

Summary “Bins” of Protective Measures Identified



Hypothetical Scenario 1: Theft of Valuable Intellectual Property (1)

- A revolutionary anti-cancer biotherapeutic, Tumex, based on a human immune system protein, was discovered by NuGene Therapeutics, Inc. During Phase I clinical studies, Tumex was found to be exceptionally efficacious and was soon recognized as potentially a “blockbuster” therapeutic due to its effects on even advanced stage solid tumors. (“Blockbuster” status indicates the drug is projected to generate annual sales of ≥$1B)
- The one issue facing NuGene Therapeutics is that the therapeutic is very unstable after injection. The high doses required to maintain therapeutic levels causes toxicity. However, the therapeutic dose for efficacy is quite low, so developing a more stable derivative would be invaluable. After intensive research to overcome the stability issue NuGene identifies a derivative that is 100-fold more stable and retains full efficacy – NuGene’s stock price soars on the news. NuGene contracts with Process Development, Inc. (PDI) for process development and scale-up of the revised therapeutic, TumexPlus.

Hypothetical Scenario 1: Theft of Valuable Intellectual Property (2)

- PDI specializes in expression of biotherapeutics in a yeast system, *Pichia pastoris*, and is provided the amino acid sequence of TumexPlus by NuGene Therapeutics so an expression system can be developed. PDI designs the TumexPlus coding sequence for insertion into their proprietary Pichia expression system. To do so, the lead molecular biologist at PDI uses internet-based software to develop a codon-optimized DNA sequence to express TumexPlus in Pichia.
- The codon-optimized sequence is then perfected in-house for nearest-neighbor codon usage and other expression factors using PDI proprietary software, appropriate restriction sites are appended to each end of the coding sequence for ease of cloning, and synthesis of the final DNA sequence is ordered over the internet.

Hypothetical Scenario 1: Theft of Valuable Intellectual Property (3)

- Unknown to the molecular biologist and others at PDI, the laptop used for molecular design was compromised during use at a trade show attended by the molecular biologist. During the show, a shadowy hacking consortium, Primo Hack (PH), was able to corrupt thumb drives that were going to be handed out by a new company who has been generating a lot of interest in the field lately. The molecular biologist inserts the infected thumb drive in his laptop. While it includes information that he is interested in, it also drops a malware payload on the laptop.
- All data generated and stored on the laptop is being monitored and collected by PH hackers. They quickly stole and sold the PDI proprietary gene design software. When they discover they have the sequence of TumexPlus, they know they hit the mother lode. They quickly send out feelers to potential buyers who just as quickly start a bidding war for the data. Pharma Bro, a buyer with deep pockets that they have dealt with in the past wins the bidding war and takes possession of the proprietary data for a paltry $870K.

Hypothetical Scenario 1: Theft of Valuable Intellectual Property (4)

- Pharma Bro's operation is international with facilities in India, China, and Latin America. Production in all three locations is immediately directed towards producing TumexPlus which is produced, formulated and sold under the brand name, "Lumpaway". Pharma Bro's previous dealings with regulatory agencies in all three locales guarantee "approval" of his new drug without delay. Lumpaway grabs market share on the international market while TumexPlus is still only midway through clinical trials.
- Once TumexPlus is finally approved by the US FDA and European Medicines Agency and goes on the market, the stolen biotherapeutic "copy" brand name is well embedded in the market. Revenue generated by TumexPlus is severely depressed relative to projections and the value of NuGene Therapeutics stock takes a major loss. Pharma Bro's return on investment exceeds $1B per year while legal challenges by NuGene Therapeutics to ownership rights drag on for years in their country's civil court system.

Hypothetical Scenario 2: Compromise of the Supply Chain (1)

- Ahso Biotherapeutics and Omega Biopharma have been in a very competitive relationship over several years as each seeks to bring an anticoagulant therapeutic to market. Previous anticoagulants developed by large pharma companies had just failed clinical trials. Both companies had non-exclusively licensed the rights to commercialize a molecule developed at a regional University that did not have non-specific activity that caused the large pharma products to fail. Delays in commercialization were encountered by both and the financial futures of both were dependent on success with this product.
- Ahso had sufficient financial backing but lack of scientific expertise slowed progress. In contrast, Omega had trouble generating investor interest but finally secured the funding needed. Although development was slowed at Ahso, they were well ahead of Omega and were transitioning the anticoagulant to their Biological Process Development Facility (BPDF). Realizing the precarious competitive position in which they find themselves, Omega engages an “attacker” group with the needed expertise to hack into the Ahso online procurement system, eSHOP, and the Ahso email system.

Hypothetical Scenario 2: Compromise of the Supply Chain (2)

- The attacker group identifies an employee who regularly works on eSHOP approvals while waiting for their drink and lunch at Starbucks. The attacker group set up a man-in-the-middle attack by spoofing the Starbucks free Wi-Fi to capture the user's password. The user has no idea that their password has been compromised. The attacker group can use the login information at their leisure.
- Using passive surveillance, the attackers piece together task schedules and procurement patterns. They identify billing codes that are displayed prominently for all eSHOP purchases and correlate them to projects; and, they scrutinize email traffic for information that may be useful in disrupting the Ahso project.

Hypothetical Scenario 2: Compromise of the Supply Chain (3)

- All the information is evaluated and it becomes clear that Omega must cause significant disruption to the Ahso project in order for them to get to market first with the anticoagulant. Close analysis of all the data, and in close consultation with Omega, the attackers decide the most disruptive and time-consuming event would be to contaminate the product near the end of manufacture.
- They consider several approaches: contaminating bioprocess bags with bacterial spores but decided it would only cause short-term delays during decontamination and may not set the project back enough; spiking a highly toxic compound into a reagent which might debilitate BPDF staff which would be quickly recognized as sabotage even if effective; and, lastly, they consider and settle on a somewhat more subtle approach to introduce Bacillus anthracis spores in the storage containers used for bulking the final product.

Hypothetical Scenario 2: Compromise of the Supply Chain (4)

- The attackers learned that the final product would be bulked into 125 mL sterile bottles for shipment to a fill/finish facility. By chance, a relative of one of the attackers works for a local logistics company that routinely delivers packages to the Ahso facility. By monitoring eSHOP, the attackers knew when and exactly which storage bottles were ordered; their insider intercepts them at the logistics warehouse. They cover their delay by sending an email to Ahso indicating the bottles were on back order and would be delivered a week late.
- The intercepted bottles were unpackaged carefully, uncapped and each contaminated with approximately 1 million *Bacillus anthracis* spores. After capping and resealing the bottles so they appeared unopened and sterile, they are delivered to the BPDF. The bottles were checked in, quarantined and delivered to the GMP suite as normal. Once purified and adjusted to the desired concentration in the appropriate buffer, anticoagulant samples are collected for stability studies and for release testing.

Other Realizations During the Project

- The Cyberbiosecurity Paradigm could be applied more comprehensively across biomanufacturing and across a number of complex sectors for which life science activities, systems and technologies are dependent upon or interfaced with information technologies/systems or cyber-physical systems
- It is likely that insufficient attention is being applied to potential and existing threats and developing and implementing solutions, no matter the sector
- Simple, relatively straightforward measures exist and could be adopted to "raise the bar" (at least somewhat) against adversaries operating in this ecosystem
- No "authority", or organizational construct, exists to promote "Cyberbiosecurity"; thus, a "good, old fashioned, grass roots campaign" is required to raise awareness and organize a Community of Interest, at least for for the foreseeable future
- **To be effective, Cyberbiosecurity analyses and outcomes require a convergence of experts, perspectives and resources, i.e., it's definitely not only "this is just cybersecurity applied to biological (biomedical) activities, systems & infrastructures"**
- Technology and technical methods alone will not be sufficient to address current and future threats in this venue; a "kit of tools" is required, not just technological but including assessment training, guidelines/standards, response and resolution protocols
- Some problems/threats exist with require specialized, advanced, "lean way forward" research investments

“Cyberbiosecurity” Has Been Created, Is Rapidly Expanding and “the Story” Unfolding!!

- Definition:
  - Emerging discipline which exists at interface of cybersecurity and biosecurity
  - Seeks understanding of the vulnerabilities to unwanted surveillance, intrusion, malicious, and harmful activities, which can occur within or at the interfaces of comingled life sciences, cyber-physical, and infrastructure systems
  - Seeks to discover, develop and implement measures to prevent, protect against, mitigate, investigate, and attribute such threats.
    - Adapted from: Murch, R. S., K. L. W. So, S. Raman, W. Buchholz and J. Peccoud. 2018. **Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy.** Front. Bioeng. Biotechnol. Vol. 6, Article 39, 6 ppg. DOI: 10.3389/fbioe.2018.00039
- Active Engagement: USG Agencies and Offices Already Demonstrating Interest -- FBI, ODNI and IC Agencies, Many components in DoD; and, expanding into NIST, FDA, USDA, NSC, OSTP
- Presentations at professional societies, one National Lab, many loci within USG and to USG advisory groups

- Peccoud, J., Gallegos, J., Murch, R., Buchholz, W., Raman, S. 2017. **Cyberbiosecurity in Biotechnology: Trading Trust for Awareness.** Trends in Biotechnology, DOI: http://dx.doi.org/10.1016/j.tibtech.2017.10.012
- Murch, R. S., K. L. W. So, S. Raman, W. Buchholz and J. Peccoud. 2018. **Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy.** Front. Bioeng. Biotechnol. Vol. 6, Article 39, 6 ppg. DOI: 10.3389/fbioe.2018.00039
- Murch, R. S., D. DiEuliis, Editors. Research Topic Special Collection, “**Mapping the Cyberbiosecurity Enterprise**”, published in **Frontiers: Bioengineering and Biotechnology (Biosafety and Biosecurity)** beginning late Winter 2019
  - https://www.frontiersin.org/journals/bioengineering-and-biotechnology/sections/biosafety-and-biosecurity#research-topics
  - Thus far ca. ~16 articles supported by >65 Authors expected
  - Currently 16 manuscripts received, 5 published, 2 imminent, 2-3 expected to be published soon, the remainder by June
  - Titles of published articles
    - **Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System**
    - **Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience**
    - **The National Security Implications of Cyberbiosecurity**
    - **National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data**
    - **Defending our Public Biological Databases as a Global Critical Infrastructure**
  - Next to be published:
    - **Next Steps for Access to Safe, Secure DNA Synthesis**
    - **Cyberbiosecurity: a call for cooperation in a new threat landscape**
  - >8300 views as of 4/22/19

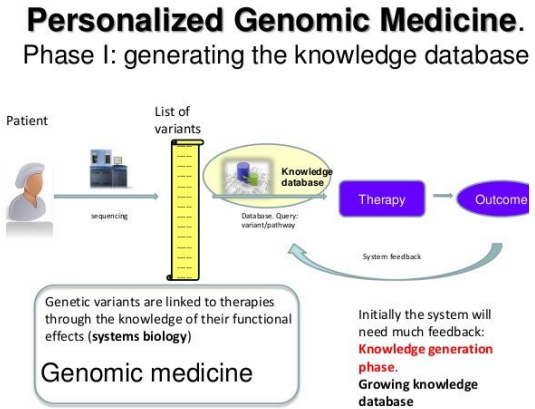
- **All of this is being viewed and pursued as being integral to “Safeguarding the Bioeconomy”**

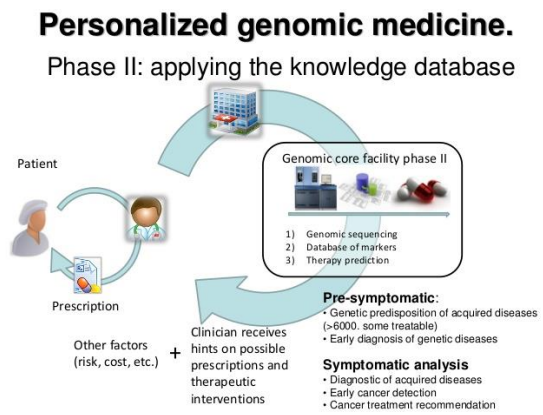
What Potential Vulnerabilities in Exist for Synthetic Biology Activities, End to End?

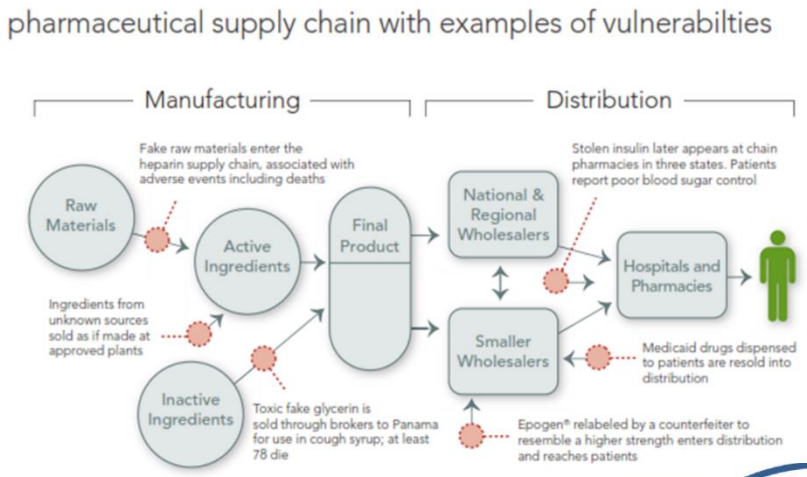
- What can be learned from the analysis of the biomanufacturing facility, and other reports and work, that could be applied to synthetic biology activities/facilities?
  - Are there similarities?
  - Are there differences?
- Are there any differences with respect to vulnerabilities from the cyberbiosecurity viewpoint that present for synthetic biology that do not present for genetic engineering?
- What do we understand about the array of adversaries that may be encountered and how each would approach targeting → realizing objectives/outcomes (including “Plan B”)?
- Can cyberbiosecurity-mediated threats and mitigations/solutions for synthetic biology (genetic engineering) be anticipated and modeled?
- How do we organize, prioritize and pursue understanding and implementation of threats, manifestations and defenses?

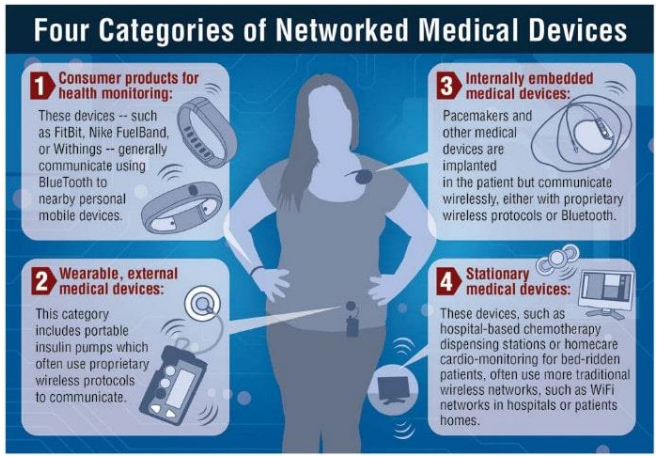
Some Possible Steps on the Path Forward

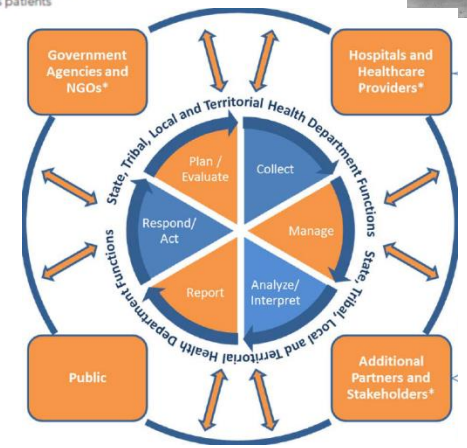
- Include synthetic biology in the cyberbiosecurity discussions, including through peer-reviewed publications and presentations to interested audiences (including biomanufacturing)
- Convene a series of structured national and international meetings with the "just-right blended" expertise to, e.g.:
  - Increase Awareness, Educate
  - Establish a Community of Interest
  - Agree on Common Vernacular/Terms of Reference
  - Generate Common Set of Plausible, Hypothetical Scenarios for Benchmarking
  - Initiate the Development and Validation of Priorities through A Structured Approach
    - Science & Technology, Practices, Policy & Regulatory, Studies & Analyses, Training
    - Guidelines (or Standards) Might Be Among the First
  - Perform "Deep Dives" in Specific Areas for Which Greater Understanding is Required to Inform Perspectives and Decisionmaking
  - Identify & Recruit Leadership (Government, Non-Government) to Carry Forward
  - Explore & Agree Upon Follow On Activities & Actions
- Engage Policy Makers, Key Decision Makers & Influencers in Other Sectors

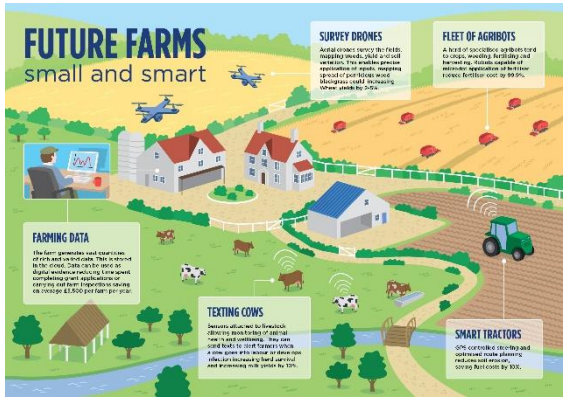












Randall (Randy) Murch, PhD,
Research Lead and Professor,
Virginia Tech, rmurch@vt.edu