The Emergence of Cyberbiosecurity

Randall Murch, PhD
Virginia Tech
Health Security Partners & Brazilian SB3 Conference
August 24-25, 2022

Context for Today's Presentation

- **I have worked in aspects of the field of what is now Biosecurity since mid-1990s**
- **Biosecurity is a field which is focused on minimizing the risk of misappropriation and misuse of pathogenic disease agents and biological toxins.**
  - **There are many aspects to this field, including forensics and attribution of biothreats (my specialty)**
- **Since its origin until the present, Biosecurity continues to focus on the policies, practices, treaties, laws, public health effects and international and national cooperation to advance risk mitigation**
- **In the last 7+ years, there has been a emerging realization that view of Biosecurity must be widened…**

Publications & Activities That Helped Lay The Foundation for a New Field "Cyberbiosecurity"

- American Association for the Advancement of Science, Federal Bureau of Investigation and United Nations Interregional Crime and Justice Research Institute. 2014. **National and Transnational Implication of Security of Big Data in the Life Sciences.** . American Association for the Advancement of Science, Washington, DC. 91 ppg
- Three National Academies Workshops 2014 – 2016 and Reports
  - **Convergence: Safeguarding Technology in the Bioeconomy (2014)**
  - **Safeguarding the Bioeconomy II: Applications and Implications of Emerging Science (2015)**
  - **Safeguarding the Bioeconomy III: Securing Life Sciences Data (2016)**
- Pauwels, E. and Vidyarthi, A. 2016. **How Our Unhealthy Cybersecurity Infrastructure is Hurting Biotechnology**. Wilson Briefs, March 2016. The Wilson Center, Washington, DC, 4 ppg
- Pauwels, E. and Vidyarthi, A. 2017. **Who Will Own the Secrets in Our Genes? A U.S. – China Race in Artificial Intelligence and Genomics**. Wilson Briefs, February 2017. The Wilson Center, Washington DC, 14 ppg
- Pauwels, E and Dunlap, G. 2017. **The Intelligent and Connected Bio-Labs of the Future: The Promise and Peril in the Fourth Industrial Revolution.** 2017. Wilson Briefs, September 2017. The Wilson Center, Washington, DC, 17 ppg
- Kozminski, K. G. and Drubin, D. G. 2015. **Biosecurity in the Age of Big Data: A Conversation with the FBI.** Mol. Biol. Cell 26 (22): 3894-3897, doi: 10.1091/mbc.E14-01-0027
- You, E. H. 2017. **Safeguarding the Bioeconomy: U.S. Opportunities and Challenges**. Testimony for the U.S. – China Economic and Security Review Commission, Washington, DC, March 16, 2017

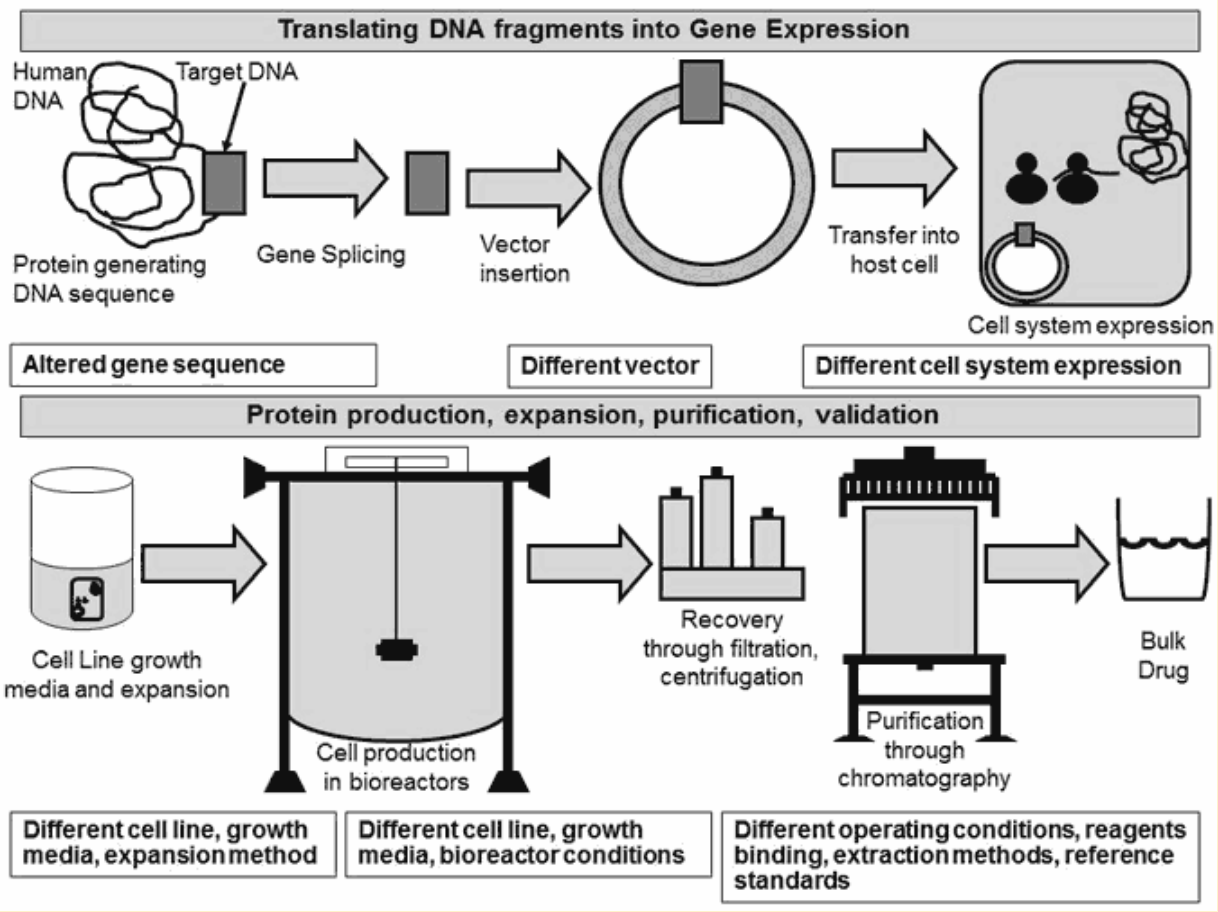
Origins of Cyberbiosecurity, Original Project

- Complete agreement with premise that biosecurity too pathogen-focused, must be more expansive
- Concept created and developed by three then-Virginia Tech faculty (two left for positions in other universities, one still at Virginia Tech, VT)
- Funding was successfully obtained from a US Government sponsor, 1 Year Period of Performance
- An ideal biological process development facility was identified
- Three-university study team created: R. Murch (VT) was the Principal Investigator (PI)
- Project: One-year comprehensive systems analysis to identify vulnerabilities to compromise, most of the vulnerabilities have a IT component
- **Systems Analysis, Not an R&D project; Facility was not compromised or "hacked"; Analysis conducted from the systems-of systems perspective**

Summary of Original Project

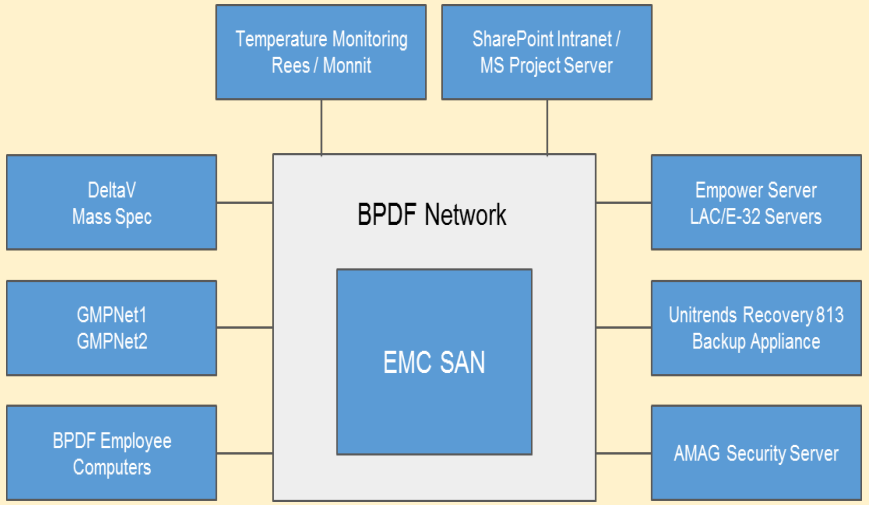
- Comprehensive systems analysis of a bioprocess development and production facility at a university in the midwestern U.S.
- Facility was benignly studied in depth, not “hacked or corrupted”
- Four major area of focus:
  - **Bioprocess development and scale up**
  - **Information systems infrastructure, including that which supports the above**
  - **Supply chain, into and from the facility**
  - **Hypothetical and plausible scenarios**
  - Final Report
- Blended Team: PI with Wide Dynamic Range of Expertise including Systems Analyses; Facility Director from Similar Facility (University of Nebraska) with Complementary Skills to PI; Genomics/Bioinformatics (Colorado State University); Technical Experts, Including IT Admin and Procurement Lead (University of Nebraska, Cyber/IoT Security (Virginia Tech)

Cyberbiosecurity was Initially Defined and Developed Using a Biomanufacturing Model

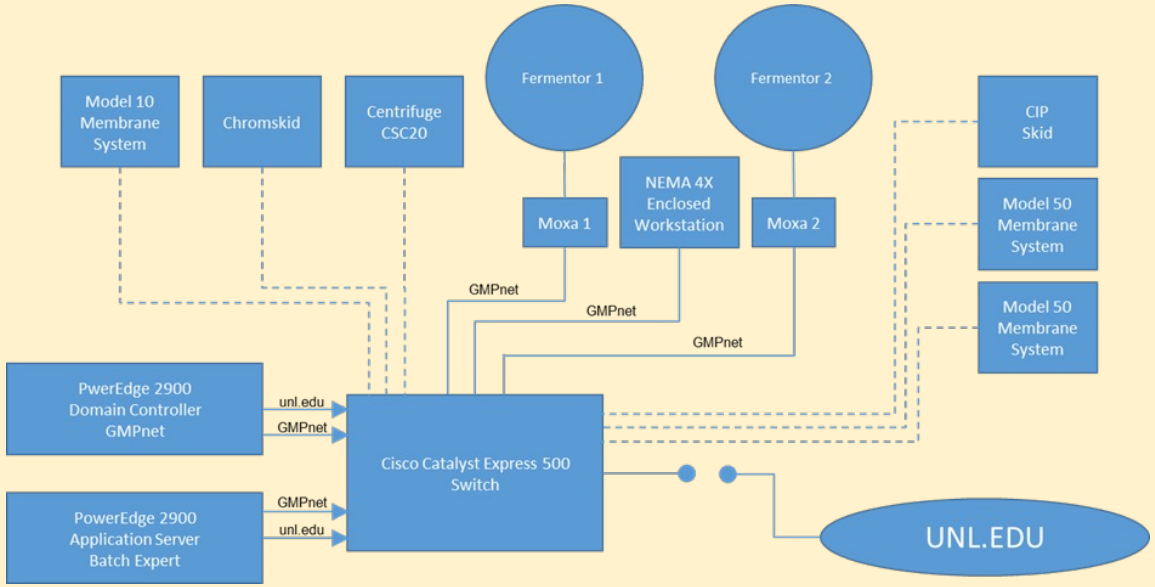


- **Specialty proteins are designed through designing specific genetic segments that are used to derive the desired product.**
- **The fully tested product is sent to a customer with all of the technical documentation. This is usually further tested in clinical trials before going to market.**

Bioprocess Development and Biomanufacturing is Supported by an Information System Infrastructure

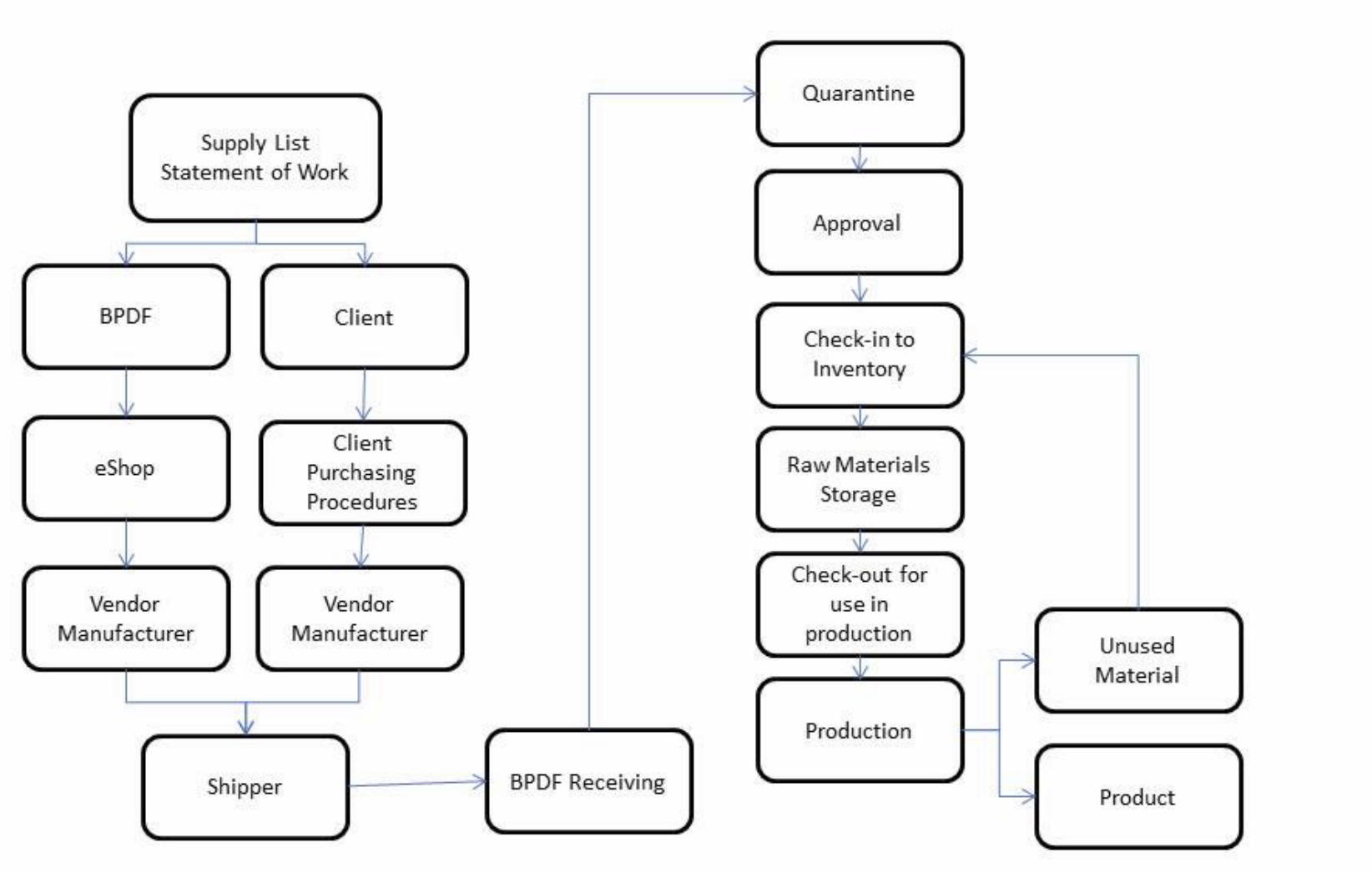


High-level depiction of the Bioprocess Development Facility (BPDF) Information System Infrastructure Studied



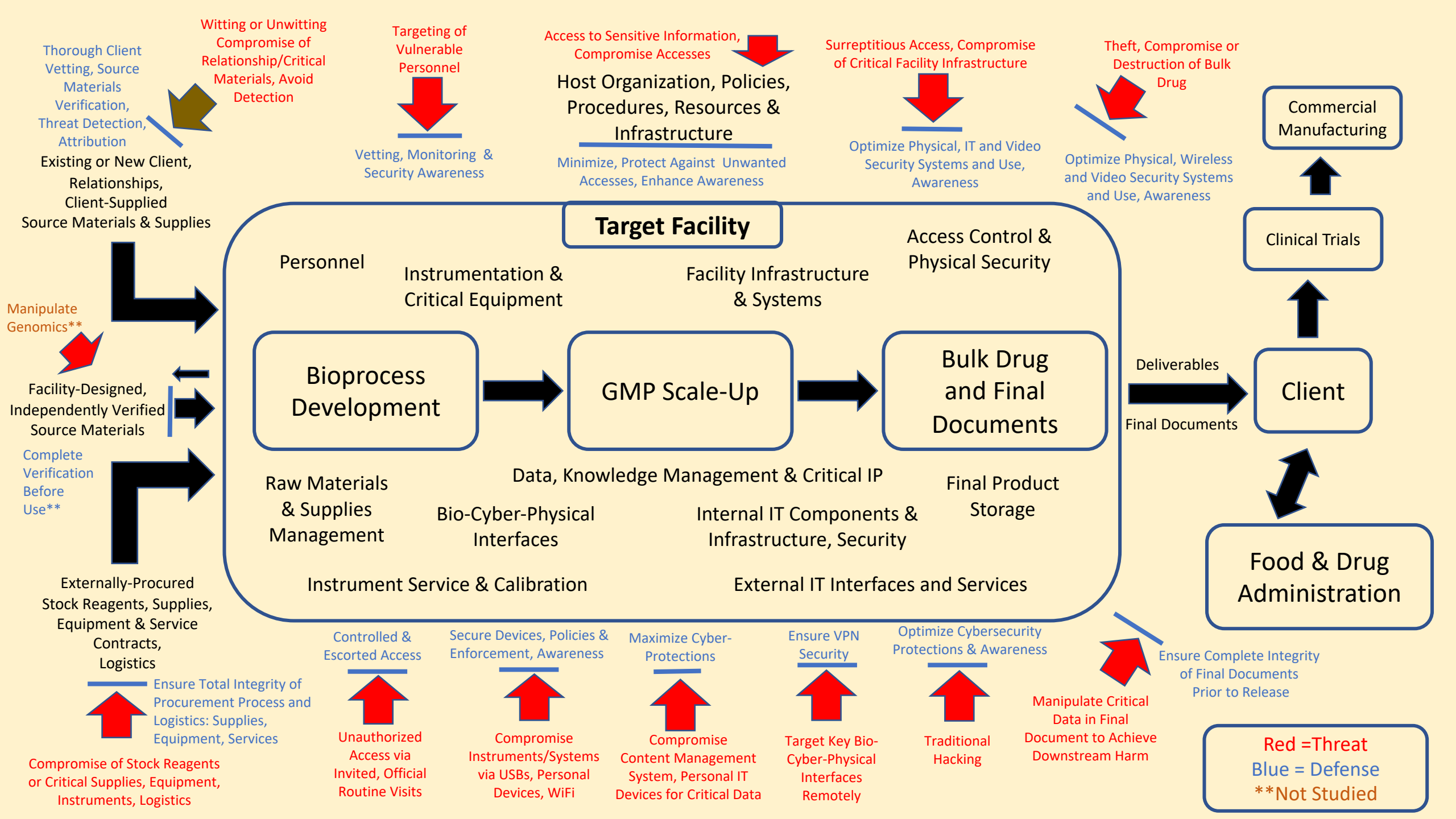
High-level Depiction of the GMP Facility Network Studied

Additionally, our team developed a series of "subsystems models" for each component of mid-scale Bioprocess Development and Biomanufacturing to identify the most critical components, nodes and links in preparation for deep characterizations to inform preventive, protective and response measures



Bioprocess Development & Biomanufacturing is a "System of Systems"

"Supply Chain": Process for acquisition of equipment, instruments, raw materials and consumables --- procurement, receipt, set up and storage until use.


Thorough Client Vetting, Source Materials Verification, Threat Detection, Attribution
Witting or Unwitting Compromise of Relationship/Critical Materials, Avoid Detection
Existing or New Client, Relationships, Client-Supplied Source Materials & Supplies
Targeting of Vulnerable Personnel
Vetting, Monitoring & Security Awareness
Access to Sensitive Information, Compromise Accesses
Host Organization, Policies, Procedures, Resources & Infrastructure
Minimize, Protect Against Unwanted Accesses, Enhance Awareness
Surreptitious Access, Compromise of Critical Facility Infrastructure
Optimize Physical, IT and Video Security Systems and Use, Awareness
Theft, Compromise or Destruction of Bulk Drug
Optimize Physical, Wireless and Video Security Systems and Use, Awareness
Commercial Manufacturing
Clinical Trials
Target Facility
Personnel
Instrumentation & Critical Equipment
Facility Infrastructure & Systems
Access Control & Physical Security
Manipulate Genomics**
Facility-Designed, Independently Verified Source Materials
Complete Verification Before Use**
Bioprocess Development
GMP Scale-Up
Bulk Drug and Final Documents
Deliverables
Final Documents
Client
Raw Materials & Supplies Management
Data, Knowledge Management & Critical IP
Bio-Cyber-Physical Interfaces
Internal IT Components & Infrastructure, Security
Final Product Storage
Instrument Service & Calibration
External IT Interfaces and Services
Externally-Procured Stock Reagents, Supplies, Equipment & Service Contracts, Logistics
Food & Drug Administration
Ensure Total Integrity of Procurement Process and Logistics: Supplies, Equipment, Services
Compromise of Stock Reagents or Critical Supplies, Equipment, Instruments, Logistics
Controlled & Escorted Access
Unauthorized Access via Invited, Official Routine Visits
Secure Devices, Policies & Enforcement, Awareness
Compromise Instruments/Systems via USBs, Personal Devices, WiFi
Maximize Cyber-Protections
Compromise Content Management System, Personal IT Devices for Critical Data
Ensure VPN Security
Target Key Bio-Cyber-Physical Interfaces Remotely
Optimize Cybersecurity Protections & Awareness
Traditional Hacking
Manipulate Critical Data in Final Document to Achieve Downstream Harm
Ensure Complete Integrity of Final Documents Prior to Release
Red =Threat
Blue = Defense
**Not Studied

Examples of Possible Cyberbiosecurity Threats

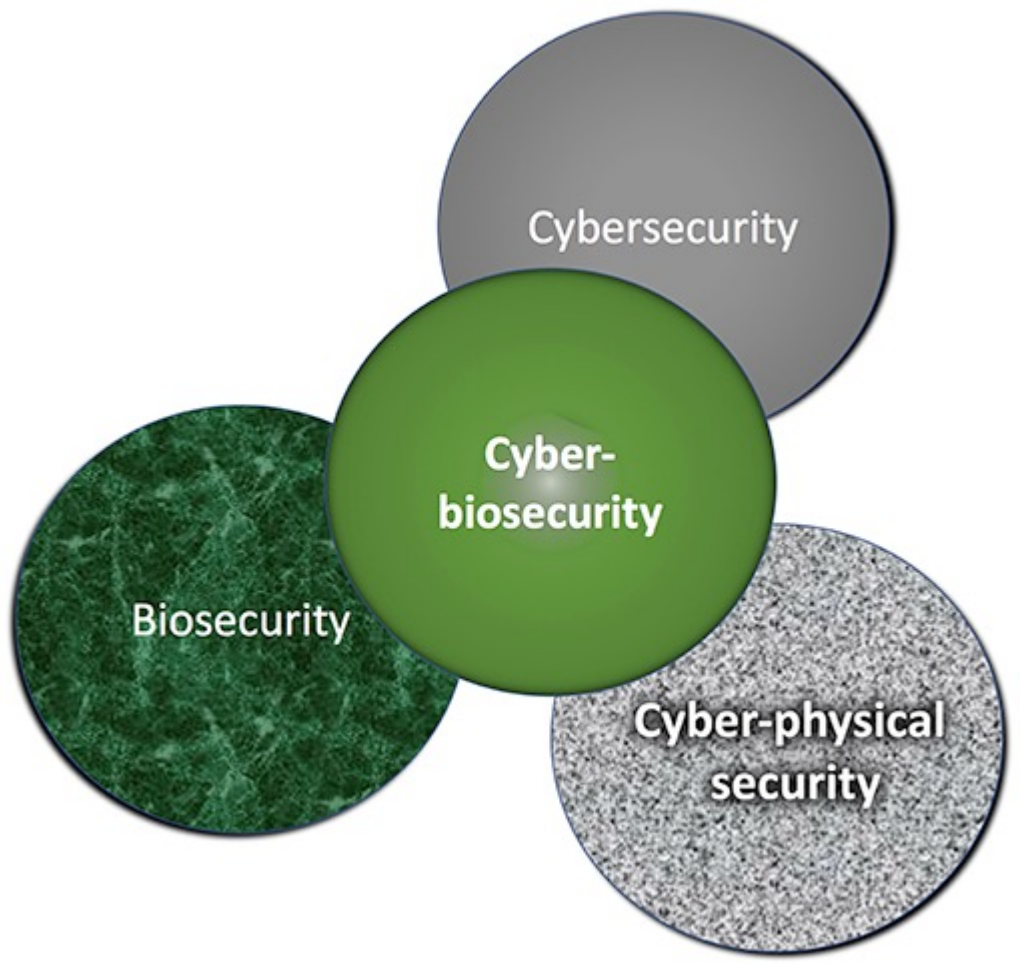
- **Stealth electronic monitoring of facility activities and information that result in the theft of intellectual property**
- **Exploiting weaknesses to facilitate other unwanted incursions or intrusions**
- **Corruption of key aspects of bioprocess development or biomanufacturing resulting in a suboptimal 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 effects**

Some Possible Cyberbiosecurity System Vulnerabilities in High Biocontainment Labs?

- **Unwanted Access to and Theft of Intellectual Property?**
- **Corruption of Laboratory Experimental Data or Data Analytics?**
- **Unwanted Monitoring or Hacking of Electronic Communications?**
- **Undetected Manipulation or Corruption of Critical Stored Data and Metadata?**
- **Unwanted Access to and Manipulation of Cyber Physical Interfaces (e.g., Networked or Remotely Accessed Instrumentation)?**
- **Monitoring of Procurement Actions Which Could Lead to Compromise of Integrity of Supply Chain?**
- **Degradation of Facility Access Security Systems?**
- **Others (e.g., Inducing Failures in Environmental Monitoring and Control Systems)?**

Sponsor Position, First Workshop and Initial Publications

- **During outbrief** and the university team's final involvement (September 2017), **the U.S. Government Sponsor expressed their very substantial pleasure and excitement with the results**
- The Sponsor urged the academic team to **"go as far and fast as we could with the concept, the approach and possible related pursuits"**
- **Virginia Tech, Colorado State and Two Companies Sponsored Workshop at VT, October 2017**, ~45 attendees, which included **8 US Government agencies, 10 academic institutions including the National Academies of Science, Engineering and Medicine, two pertinent non-profit organizations, four companies** (including two which were sponsors of the event*)*
- Two initial publications:
  - **Peccoud, J., J. Gallegos, R. Murch, W. Buchholz and S. Raman. 2017. Cyberbiosecurity: From Naive Trust to Risk Awareness. Trends in Biotechnology, 36 (1): 4-7, 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**



Cyberbiosecurity Definition

Developing understanding of vulnerabilities, then design and implement effective countermeasures:

- **Identifying and characterizing unwanted surveillance, intrusions, malicious and harmful activities**
  - **which can occur within or at the interfaces of comingled life sciences, cyber-physical and IT infrastructure systems**

- **Developing measures to prevent, protect against, mitigate, investigate and attribute such threats.**

Duncan, S. E. et al, Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System. Front. Bioeng. Biotechnol., 29 March 2019| https://doi.org/10.3389/fbioe.2019.00063

Murch, R. S. et al. 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

The E-Book: “Mapping the Cyberbiosecurity Enterprise”

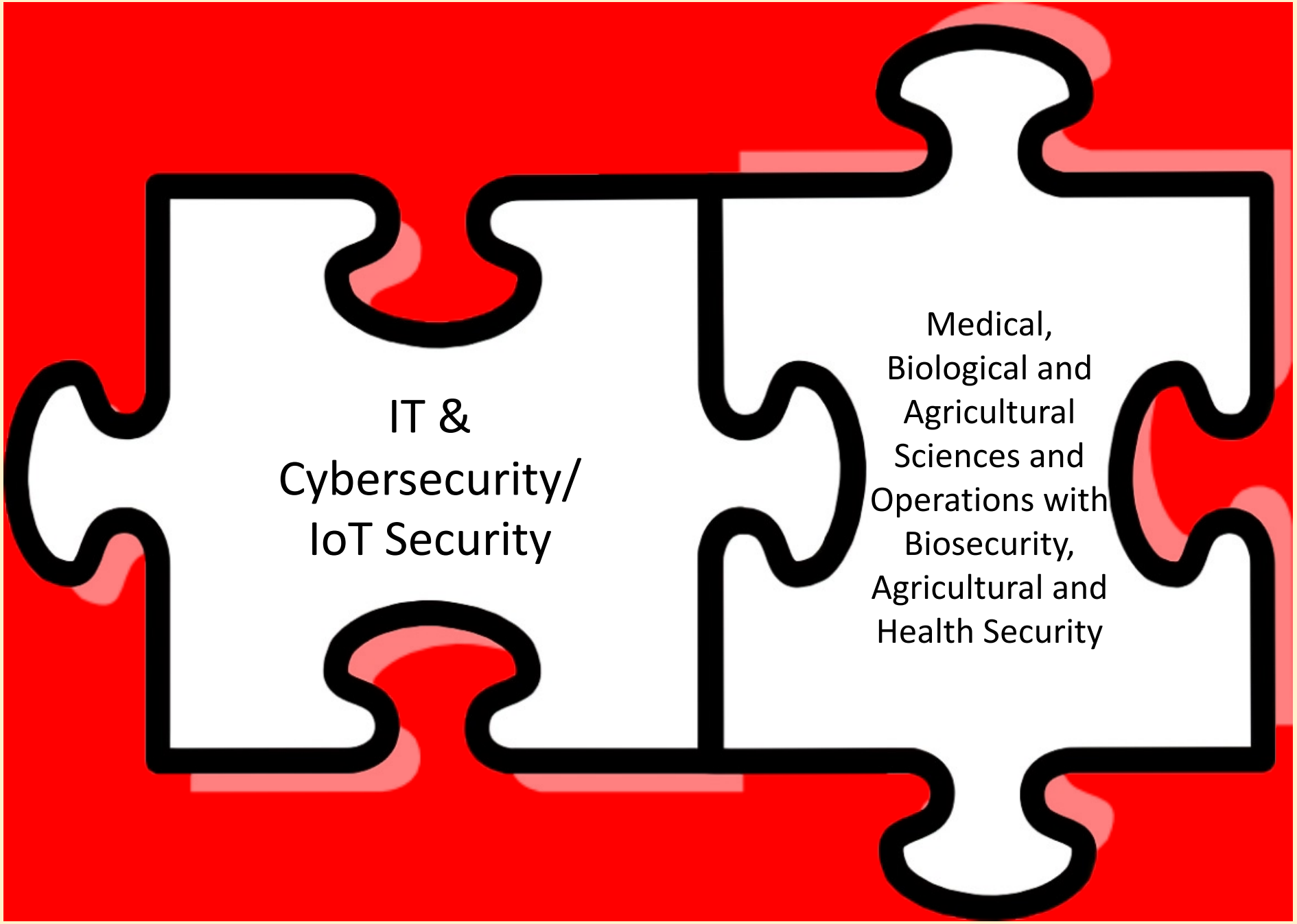
- Due to the previous publication in **Frontiers in Bioengineering and Biotechnology (Section on Biosafety and Biosecurity**) and role as Associate Editor of that section, the Editor asked me to put together an e-book on Cyberbiosecurity
- My colleague Dr. Diane DiEuliis, National Defense University, and I were co-Editors
- Finally published in early October 2019; 16 articles, 71 authors
- **https://www.frontiersin.org/research-topics/8353/mapping-the-cyberbiosecurity-enterprise**, download pdf or E-Pub
  - Also published as a Google book
- **As of the morning of July 21, 2022, there were 113,425 views, 92,028 article views, 16,206 article downloads and 5,134 topic views; usually increases at least several hundred per week. Demographics literally wrap all around the globe**
- Many follow-on pubs and citations from across the globe, including from Virginia Tech in other venues (e.g., IEEE journals)
- **New books are underway, one being led by a professor at Yale University USA, one being led by faculty at the University of Edinburgh, Scotland UK**

++

- **In addition to all of the aforementioned, I have given >20 presentations to a variety of audiences both within the U.S. as well as other countries, small groups to highly public settings and high-level audiences**

Possible Paths Forward (Examples)

- Develop a strategy and execute to build and maintain national, regional or worldwide community
- Identify specific projects that can be pursued through national, regional or international teams to strengthen the security of categories of laboratories
- Develop and implement an international certification program for cyberbiosecurity specialists in laboratories (underway)
- Expand the cyberbiosecurity approach to other applications (e.g., cloud computing, AI, synthetic biology, data analytics) (You will soon meet my colleague Dr. Feras Batarseh)
- Develop the “next generation” (students)


IT &
Cybersecurity/
IoT Security
Medical,
Biological and
Agricultural
Sciences and
Operations with
Biosecurity,
Agricultural and
Health Security

Center for Advanced Innovation in Agriculture

- **Virginia Tech's College of Agriculture has recently created a new center, named the Center for Advanced Innovation in Agriculture (CAIA, pronounced "Kai-Ya") which focuses on:**
  - Smart Farms
  - **Cyberbiosecurity**
  - Data Analytics
- **Ca. 110 Faculty from across the College of Agriculture and Life Sciences, and other Colleges in the University**
  - **Major Webinar in Fall of 2020**
  - **CAIA Day 2022**
  - **Publishing, Initiating Research, Developing Outreach and Education Approaches, and Pursuing Grants**
  - **Strong Relationships with a Major IT-Research Program in the Commonwealth of Virginia, named the Commonwealth Cyber Initiative which has several Virginia universities involved and is funded by the Commonwealth of Virginia government as well as through research contract and grants.**

If Interest Exists in Brazil…

- Who will be the champions for cyberbiosecurity in Brazil?
- What sectors in Brazil might benefit most from cyberbiosecurity?
- What is necessary for Brazil to develop and implement a national program in cyberbiosecurity?
- What would a strategy for cyberbiosecurity in Brazil look like?
- How should research, systems analysis, development, test, validation and implementation be supported and shared in Brazil?
- What Brazilian Government agencies or entities should be engaged to support and advance cyberbiosecurity?

Questions and Discussion