Cyberbiosecurity–A Compilation of Summaries of Peer-Reviewed Publications, Government Publications, and Relevant Resources.

Compiled and summarized by Rachel Mack[1] and Rebekah Miller[2]

[1]Ph.D. Candidate, Agricultural, Leadership, and Community Education, Virginia Tech, Blacksburg, VA

[2]MSLFS Student, Food Science & Technology, Virginia Tech, Blacksburg, VA

This compiled list of summaries and resources includes 81 sources which together represent the current knowledge base on cyberbiosecurity resulting from the workshop, *Securing Agriculture, Food, and its Economy (SAFE) with Cyberbiosecurity*,[3] held virtually on October 6-7, 2020. These resources include peer reviewed publications, relevant papers, government documents and publications, and press releases. Funding for these summaries and the workshop provided by USDA-NIFA Grant No. 2019-67021-29956, Accession No. 1019771, the Virginia Agricultural Experiment Station, the Virginia Commonwealth CyberInitiative Southwest Node, and Tyson Foods.

Resources Summarized in this Document

Bedord, L. (2016, April 5). Midwest Agriculture Is A Prime Target For Theft Of Intellectual Property And Cyber Attacks. *Successful Farming*.

Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. *Frontiers in Bioengineering and Biotechnology*, *7*, 21.

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer*, *52*(3), 58-66.

[3] https://www.cpe.vt.edu/cyberbiosecurity/index.html

Bipartisan Commission on Biodefense. (2015). *A national blueprint for biodefense: Leadership and major reform needed to optimize efforts – Report of the Bipartisan Commission on Biodefense*. Washington, DC: Hudson Institute.

Bipartisan Commission on Biodefense. (2017). *Special focus: Defense of animal agriculture*. Washington, DC: Bipartisan Commission on Biodefense.

Caswell, J., Gans, J. D., Generous, N., Hudson, C. M., Merkley, E., Johnson, C., Oehmen, C., Omberg, K., Purvine, E., Taylor, K., Ting, C. L., Wolinsky, M., & Xie, G. (2019). Defending our public biological databases as a global critical infrastructure. *Frontiers in Bioengineering and Biotechnology*, *7*, 58.

Chabrow, E. (2011). Creating Ag Extension Agent for Cyber: Championing a new way to spread infosec awareness. *Gov Info Security*.

Corteva Agriscience (2020, April 29). *MercyOne and Corteva Agriscience Join Forces to Increase COVID-19 Sample Testing*.

Daniels, K. (2020). Researchers apply new technology to identify plant pathogen strains in Virginia. *Virginia Tech Daily*.

Diggans, J., & Leproust, E. (2019). Next steps for access to safe, secure DNA synthesis. *Frontiers in Bioengineering and Biotechnology*, *7*, 86.

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting us food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, *7*, 63.

Durrell, K. (2019). The buzz around insect protein: Protix inaugurates €45 million facility in the Netherlands. *Food Ingredients First*.

Engelking, C. (2019, March 19). Edible Insects Are The New Animal Farm. *Discover Magazine*.

FDA. (2020, July 30). 2020 Leafy Greens STEC Action Plan. Retrieved from https://www.fda.gov/food/foodborne-pathogens/2020-leafy-greens-stec-action-plan

Gaffney, J., Schussler, J., Loffler, C., Cai, W., Paszkiewicz, S., Messina, C., Groeteke, J., Keaschall, J., Cooper, M. (2015). Industry-Scale Evaluation of Maize Hybrids Selected for Increased Yield in Drought-Stress Conditions of the US Corn Belt. *Crop Science, 55*(4).

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agricultural industry. *International Food and Agribusiness Management Review*, *21*(1030-2018-1811), 317-334.

George, A. M. (2019). The national security implications of cyberbiosecurity. *Frontiers in Bioengineering and Biotechnology*, *7*, 51.

Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. (2019). Cyberbiosecurity in advanced manufacturing models. *Frontiers in Bioengineering and Biotechnology*, *7*, 210.

iGrow (2016). *AeroFarms Plans Largest Indoor Vertical Farm of Its Kind.*

Kozminski, K. G. & Drubin, D. G. (2015). Biosecurity in the age of Big Data: A conversation with the FBI. *Molecular Biology of the Cell, 26* (22), 3894-3897.

Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J., Schiel, J., Baker, J. C., Strychalski, E.A., Rogers, K. C., & Lee, K. H. (2019).

Cyberbiosecurity for biopharmaceutical products. *Frontiers in Bioengineering and Biotechnology*, *7*, 116.

Millett, K. K., dos Santos, E., & Millett, P. D. (2019). Cyber-Biosecurity risk perceptions in the biotech sector. *Frontiers in Bioengineering and Biotechnology*, *7*, 136.

Mueller, S. (2019). On DNA signatures, their dual-Use Potential for GMO counterfeiting, and a cyber-based security solution. *Frontiers in Bioengineering and Biotechnology*, *7*, 189.

Mulvany, L. (2019). Deere Outlook Disappoints as Trade War Keeps Farmers Frugal. *Bloomberg.*

Murch, R., & DiEuliis, D. (2019). Editorial: Mapping the cyberbiosecurity enterprise. *Frontiers in Bioengineering and Biotechnology*, *7, 235.*

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology*, *6*, 39.

National Academies of Sciences, Engineering, and Medicine. 2020. *Safeguarding the Bioeconomy*. Washington, DC: The National Academies Press.

NCC Group (n.d.). Cyber security in U.K. agriculture [PDF]. Retrieved from https://www.nccgroup.com/globalassets/our-research/uk/images/agriculture-whitepaper-final-online.pdf

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework.

Pauwels, E. and Vidyarthi, A. (2016). How our unhealthy cybersecurity infrastructure is hurting biotechnology [PDF file]. Washington, DC: The Wilson Center.

Pauwels, E and Dunlap, G. (2017). The intelligent and connected bio-labs of the future: The promise and peril in the fourth industrial revolution [PDF file]. Washington, DC: The Wilson Center.

Pauwels, E. and Vidyarthi, A. (2017). Who Will Own the Secrets in Our Genes? A U.S. – China race in artificial intelligence and genomics [PDF file]. Washington, DC: The Wilson Center.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. *Trends in Biotechnology*, *36*(1), 4.

2018 Public-Private Exchange Program (2018). Threats to precision agriculture [PDF]. Retrieved from https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision Agriculture.pdf

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology*, *7*, 99.

Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity implications for the laboratory of the future. *Frontiers in Bioengineering and Biotechnology*, *7*, 182.

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building capacity for cyberbiosecurity training. *Frontiers in Bioengineering and Biotechnology*, *7*, 112.

Schabacker, D. S., Levy, L. A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology, 7, 61*.

Schmale III, D. G., Ault, A. P., Saad, W., Scott, D. T., & Westrick, J. A. (2019). Perspectives on harmful algal blooms (HABs) and the cyberbiosecurity of freshwater systems. *Frontiers in Bioengineering and Biotechnology*, *7*, 128.

USDA (2020). USDA-NIFA and NSF establish nationwide network of artificial intelligence research institutes.

Upson, L. (2016, October 6). Introducing the Debug Project [Blog post].

Vinatzer, B. A., Heath, L. S., Almohri, H. M., Stulberg, M. J., Lowe, C., & Li, S. (2019). Cyberbiosecurity challenges of pathogen genome databases. *Frontiers in Bioengineering and Biotechnology*, *7*, 106.

Vota, W. (2020). Lessons learned measuring, evaluating, and learning with big data. Retrieved from https://www.ictworks.org/lessons-learned-measuring-evaluating-and-learning-with-big-data/#.XwkYkR17nYJ

The White House. (2012). *National Bioeconomy Blueprint*. Washington. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf

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.

Zhou, J., Reynolds, D., Le Cornu, T., Websdale, D., Orford, S., Lister, C., Gonzalez-Navarro, O., Laycock, S., Finlayson, G., Stitt, T., Clark, M. D., Bevan, M. W., Griffiths, S. (2017). CropQuant: An automated and scalable field phenotyping platform for crop monitoring and trait measurements to facilitate breeding and digital agriculture. *BioRxiv*.

Article:

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting us food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, *7*, 63.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00063/full?report=reader

Key words/potential industry:

cyberbiosecurity, protection, U.S., food, agriculture, system, life, science

Article summary:

In the U.S., issues surrounding the protection of our national infrastructure, as well as the security of our data, have been quickly changing. Food and agriculture influence a large percentage of the United States' employment and economy, and issues affecting food and agriculture can therefore affect the country on a national level. The cybersecurity of the bio economy, or the economic activity associated with technology used in generating biologically-based services and goods, must be protected. Currently, there is a need for increased and broader protection of the security of the food and agriculture system. While those in the food and agriculture industry adopt technology to remain competitive, the adoption of cutting edge technologies into the food and agriculture system create new potential threats to cyberbiosecurity. This article explores concepts related to cyberbiosecurity, highlights barriers and challenges across our food and agriculture systems, and suggests solutions for increasing cyberbiosecurity.

Article:

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. *Trends in Biotechnology*, *36*(1), 4.

Link to this article:

https://www.researchgate.net/profile/Randall_Murch/publication/321658516_Cyberbiosecurity_From_Naive_Trust_to_Risk_Awareness/links/5a65f66daca272a1582017e0/Cyberbiosecurity-From-Naive-Trust-to-Risk-Awareness.pdf

Key words/potential industry:

cyberbiosecurity, risk, awareness, trust, biotechnology

Article summary:

Biotechnology is vulnerable to many security threats. Malware can be used to attack computers, and attacks on data may be used to threaten biologically-based systems. Additionally, the space between biological systems and cybertechnology is continuing to overlap. The biotechnology field needs to adopt a culture of increased security to help avoid threats to important systems. The intersection between cybertechnology and the life sciences is not always thoroughly monitored. It is not uncommon for those in life sciences industries to operate under the expectation of self-regulation in avoiding cyberbiosecurity threats. This trust in the security of the system must change to an attitude of awareness. Awareness of cyberbiosecurity threats and support of efforts to avoid these threats are important factors for managing potential risks. Systems should work to operate with a more heightened awareness of cybersecurity vulnerabilities so that safeguards and protections may be better implemented.

Article:

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology*, *6*, 39.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2018.00039/full

Key words/potential industry:

cyberbiosecurity, emerging, bioeconomy, safeguard, biomanufacturing, life, science

Article summary:

This article introduces an expanded definition of the term ‘cyberbiosecurity,’ based on information from previous research. The term ‘cyberbiosecurity’ concerns issues from a combination of several disciplines. It describes understanding harmful activities surrounding interactions involving biological systems, cybersecurity, and physical security related to cybertechnology use. This definition will likely change over time, as cyberbiosecurity is a rapidly changing area. An important issue affecting the advancement of cyberbiosecurity is that the structure and wording used for cyberbiosecurity systems needs better identified and defined, so that points related to cyberbiosecurity can be more easily discussed and applied. Cyberbiosecurity is an important part of protecting the nation’s bioeconomy, and there are many other systems that can potentially be included in the description of cyberbiosecurity. An important opportunity exists to work on a unified structure useful for discussing and describing cyberbiosecurity.

Article:

Murch, R., & DiEuliis, D. (2019). Editorial: Mapping the cyberbiosecurity enterprise. *Frontiers in Bioengineering and Biotechnology*, *7*, *235.*

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00235/full

Key words/potential industry:

cyberbiosecurity, vulnerability, cyber-phsysical, cybersecurity, biosecurity, life, medical, science

Article summary:

This article is an editorial on the topic of cyberbiosecurity and provides an overview of key points in a group of papers included in a special edition of *Frontiers in Bioengineering and Biotechnology* titled *Mapping the Cybersecurity Enterprise*. The article addresses the many ways

that cyberbiosecurity is quickly changing. When it refers to the "mapping" of the cybersecurity enterprise, it is describing the discipline of cyberbiosecurity, how its direction has expanded, and implications that arise from this expansion. While cyberbiosecurity concerns, such as those surrounding medical data protection, have already been noted to be of importance in biomedical fields, cyberbiosecurity also has implications that cross other disciplines. The literature on cyberbiosecurity is demonstrating that the impact of cyberbiosecurity crosses many fields in the life sciences. Advances in technology bring new challenges, including reassessing cybersecurity efforts to better prepare for new threats and security issues.

Article:

George, A. M. (2019). The national security implications of cyberbiosecurity. *Frontiers in Bioengineering and Biotechnology, 7*, 51.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00051/full

Key words/potential industry:

national, security, cyberbiosecurity, risk, biodefense, government

Article summary:

This article addresses the conversation between cyberbiosecurity and national security. All countries in the world are facing risks associated with cyberbiosecurity. The biological sciences and the cyberworld are quickly merging in many ways. This merging is advantageous, as we adopt new ways of solving problems through technology, but this also increases risks to governments. The private sector and the public sector have not organized to support efforts to address cyberbiosecurity risks. This article discusses national security implications related to cyberbiosecurity. It specifically outlines ways that national security policy must address the challenges related to cyberbiosecurity. These ways include assessing risks and taking measures to guard against that risk, creating cyberbiosecurity standards with the private sector, exploring cyberbiosecurity solutions and vulnerabilities, and employing efforts from the private sector as well as all branches of government.

Article:

Schabacker, D. S., Levy, L. A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology*, *7*, *61*.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00061/full

Key words/potential industry:

cyberbiosecurity, infrastructure, resilience, vulnerability, risk management, national, security, public, private, sector

Article summary:

This article analyzes the resilience of infrastructure to cyberbiosecurity threats. New security threats have emerged as a result of the application of technology in biological contexts. The new and additional threats emerging in relation to cyberbiosecurity mean that we must develop approaches for addressing these threats. A shared approach is needed in determining vulnerabilities of systems and facilities to cyberbiosecurity threats. This paper lays out a cyberbiosecurity assessment framework. The framework addresses both resilience and security within physical and cyber contexts. The framework is built upon previous work applicable to cyberbiosecurity. The cyberbiosecurity field is complicated and presents unique problems for us to solve. The approach presented in this paper takes into account the potential to combine existing methods and capabilities from related fields, and adapt them for use in cyberbiosecurity. This can help both the public and private sectors to determine risks and vulnerabilities, while spotting options for management.

Article:

Millett, K. K., dos Santos, E., & Millett, P. D. (2019). Cyber-Biosecurity risk perceptions in the biotech sector. *Frontiers in Bioengineering and Biotechnology*, *7*, 136.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00136/full

Key words/potential industry:

cyberbiosecurity, risk, perceptions, biotech, biotechnology, biological, science

Article summary:

The biological sciences are regularly digitizing biological data. The information is both valuable on its own, and in the knowledge that can be gained through its application. The information being digitized by the biological sciences therefore needs adequately protected. A risk of not protecting this information is that lack of protection can lead to companies and countries being poorly positioned against competitors, affecting their positions in the world economy. Biotechnological infrastructure is particularly vulnerable. This is because of the use of automation, outsourcing, and distribution. Threats to biotechnological systems can be intentional or accidental. This paper describes a pilot study that gathered opinions of key players in cybersecurity and biotechnology. Results show that study participants found that cyberbiosecurity risks are varied and therefore challenging to identify. The sophistication level of response measures was also found to vary. This article calls for more research surrounding cyberbiosecurity issues.

Article:

Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. *Frontiers in Bioengineering and Biotechnology*, *7*, 21.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00021/full

Key words/potential industry:

national, international, transnational, security, biological, data, science, biotechnology

Article summary:

This article covers security issues surrounding biological data use and access. Technological advances are helping scientists in data generation, storage, and sharing. There is a large amount of data being handled by the scientific community using new and exciting technology. The data being digitized covers a wide variety of subjects in the biological sciences. Scientists can now use technology to analyze their data and find patterns in it, as well as to visualize the data. Technology also assists scientists in applying concepts from engineering to the biological sciences. Advances associated with the use of biotechnology affect numerous nations, opening the door to vulnerability to potential cyberbiosecurity threats. While various countries have policies to handle the threats to the cyberbiosecurity of their nations, top-down policies can affect data distribution among nations. This article also describes how the health sciences have been subject to threats on private data.

Article:

Caswell, J., Gans, J. D., Generous, N., Hudson, C. M., Merkley, E., Johnson, C., Oehmen, C., Omberg, K., Purvine, E., Taylor, K., Ting, C. L., Wolinsky, M., & Xie, G. (2019). Defending our public biological databases as a global critical infrastructure. *Frontiers in Bioengineering and Biotechnology*, *7*, 58.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00058/full

Key words/potential industry:

infrastructure, cyberbiosecurity, public, database, data, global, biological, science

Article summary:

The free availability of significant amounts of biology-related information in public databases is assisting in the progress of the biological sciences. This availability of data in the

public sphere is important in not just making data available to individuals, but also in advancing the pace at which scientific discovery proceeds. However, the availability of this information comes with risks. There is a trust in the security of the information. This article asserts that cybersecurity threats affecting other areas of technology will increasingly affect the security of the biological information freely available in public databases. The article calls for the proactive consideration of threats, and ways to handle them. It suggests that with this approach, we can address potential vulnerabilities before threats occur, avoiding the messiness of trying to fix problems after a cyberbiosecurity attack has already happened. This article surveys current strengths and weaknesses, and includes recommendations for managing risk.

Article:

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building capacity for cyberbiosecurity training. *Frontiers in Bioengineering and Biotechnology*, *7*, 112.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00112/full

Key words/potential industry:

cyberbiosecurity, training, information, technology, biosecurity, biological, life, science

Article summary:

Cyberbiosecurity concerns the protection of biological information and biological material. Training for dealing with cyberbiosecurity challenges must be targeted to the specific threats to an industry. To tackle challenges associated with cyberbiosecurity, consideration should be made for both the present and the future, with an eye towards increasing threat awareness. Cyberbiosecurity training and workshops are expected to combine information from both the life sciences and information technology. This training can help in identifying cyberbiosecurity threats, solutions, and assist in forming a network of interested parties. Over time, training is expected to become targeted to the specific industry in question. Information technology professionals are predicted to eventually become experts in certain areas of cyberbiosecurity, allowing for additional specialization within the information technology field.

This article discusses curricula, training, and who has interests in the development of cybersecurity training. This article also highlights current training used for managing cyberbiosecurity issues.

Article:

Diggans, J., & Leproust, E. (2019). Next steps for access to safe, secure DNA synthesis. *Frontiers in Bioengineering and Biotechnology*, *7*, 86.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00086/full

Key words/potential industry:

secure, DNA, synthesis, industry, gene, cyberbiosecurity, cybersecurity, synthetic, biology

Article summary:

This article discusses the DNA synthesis industry, security issues that it faces, and issues it could face. Best practices towards safe DNA synthesis have been created by proactive companies in the industry. These safety practices assist with the production of synthetic DNA for use in cutting edge research. These practices allow the public to benefit from safe DNA synthesis for research. However, it is useful to look at the practices being used by companies in the DNA synthesis industry to improve them. This is because the DNA synthesis industry is expanding, and new challenges associated with that expansion are expected to continue to appear. This article uses information from cybersecurity to inform practices in DNA synthesis. There are many different people involved in maintaining security of DNA synthesis, and it is important that we adapt to stay ahead of any challenges that the industry faces.

Article:

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology*, *7*, 99.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00099/full

Key words/potential industry:

cyberbiosecurity, cybersecurity, cooperation, biotechnology, healthcare, biology, information, technology, agriculture, life, science

Article summary:

Cyberbiosecurity is an important issue where the life sciences, cybersecurity, and information technology overlap. The overlap of these fields is helpful because it helps to advance the sciences. The more that biological information becomes digitized, the more that we need to consider the threats that can be linked to this digitalization. The fact that information is in a digitalized form opens the door for threats to the security of that information. This article surveys the scope of cyberbiosecurity. The article asserts that it is useful to have systems designed to be proactive to catch cyberbiosecurity threats early on. It discusses threats, and advocates for cooperation across the many fields that have cyberbiosecurity vulnerabilities. Finally, this article says that our efforts need to be aimed towards identifying cyberbiosecurity vulnerabilities and planning actions for handling those vulnerabilities.

Article:

Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. (2019). Cyberbiosecurity in advanced manufacturing models. *Frontiers in Bioengineering and Biotechnology*, *7*, 210.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00210/full

Key words/potential industry:

cyberbiosecurity, manufacturing, model, threat, biomanufacturing, industry, biopharmaceutical, healthcare, government

Article summary:

Advanced manufacturing models can help us to better access personalized healthcare through therapies targeted to assist specific patients. They can also decrease costs. However, there is concern that the advancement of the biopharmaceutical landscape could increase the potential for cyber threats. Many people are interested in maintaining safety in the production of biopharmaceuticals. These interested parties include, but are not limited to governments, healthcare workers, and associated industries. Patients are at risk of being affected by cyberbiosecurity threats, and these threats can include attacks on private patient information. Cyberbiosecurity threats to the production of biopharmaceuticals can also affect us on a global scale. This article describes cyberbiosecurity risks that could stem from advanced manufacturing systems, as well as weaknesses we currently have in our biomanufacturing structure. It shows how information often flows in biomanufacturing. Finally, it provides recommendations for handling potential cyberbiosecurity threats.

Article:

Vinatzer, B. A., Heath, L. S., Almohri, H. M., Stulberg, M. J., Lowe, C., & Li, S. (2019). Cyberbiosecurity challenges of pathogen genome databases. *Frontiers in Bioengineering and Biotechnology*, *7*, 106.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00106/full

Key words/potential industry:

cyberbiosecurity, pathogen, genome, U.S., UK, Canada, cybersecurity, database, vulnerability

Article summary:

This article discusses pathogen genome databases, with a particular interest in how cybersecurity issues, such as threats or vulnerabilities, can affect these databases. This article helps to raise awareness about cybersecurity issues affecting genome databases for pathogens, and it also suggests ways that cybersecurity can be increased, given the current weaknesses. Several countries are using whole genomes to investigate pathogens. This change towards the use of the whole genome to track a pathogen has also come with some challenges. There are

cybersecurity risks associated with the use of databases. This article suggests that the more we rely upon the use of whole genome databases, the more cybersecurity threats to those databases we could face. Cybersecurity issues raised by this article include privacy, the potential for targeted cybersecurity attacks on those identified in privacy breaches, and other challenges associated with database use.

Article:

Schmale III, D. G., Ault, A. P., Saad, W., Scott, D. T., & Westrick, J. A. (2019). Perspectives on harmful algal blooms (HABs) and the cyberbiosecurity of freshwater systems. *Frontiers in Bioengineering and Biotechnology*, *7*, 128.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00128/full

Key words/potential industry:

cybersecurity, cyberbiosecurity, freshwater, U.S., algal, bloom, water, security, system

Article summary:

This article discusses potential cyber threats to water security. It also covers ways that water security can be protected, given the various cybersecurity threats that can affect water. To this end, the article discusses harmful algal blooms, and the interesting way cybersecurity connects with these blooms. In the U.S., harmful algal blooms have been found in all 50 states, and there are many different kinds of toxins that are produced by these blooms. Human health is threatened by harmful algal blooms, so it is important that we are able to properly manage and understand them. To handle harmful algal blooms, we need to be using technology that can better inform us about them, including how to better detect them. We also need to have a system in place that can help us to respond to cybersecurity threats to the technology that predicts algal blooms.

Article:

Mueller, S. (2019). On DNA signatures, their dual-Use Potential for GMO counterfeiting, and a cyber-based security solution. *Frontiers in Bioengineering and Biotechnology*, *7*, 189.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00189/full

Key words/potential industry:

DNA, signature, GMO, genetically, modified, organism, cyber, cybersecurity, cyberbiosecurity

Article summary:

This article discusses DNA signatures and cybersecurity. It highlights major issues surrounding the use of DNA signatures, details the dilemma of DNA signature use, and addresses potential related cyber vulnerabilities. It discusses genetically modified organisms, and the possibility for their use as weapons. It also suggests that genetically modified organisms may be maliciously counterfeited. This article makes suggestions about how to enhance DNA signatures. Under the umbrella of DNA signature use, the article advocates for using both physical and digital means to protect confidentiality. Using the suggestions of the article, it is possible that we can prevent counterfeit genetically modified organisms from being distributed. This is important because counterfeit organisms may be harmful. Finally, the article says that protecting confidentiality can prevent genetically modified organism manufacturers from being blamed for the work of attackers of genetically modified organism DNA.

Article:

Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity implications for the laboratory of the future. *Frontiers in Bioengineering and Biotechnology*, *7*, 182.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00182/full

Key words/potential industry:

cyberbiosecurity, laboratory, vulnerability, risk, organization, government, economy, life, science, national, security

Article summary:

This article discusses cyberbiosecurity issues associated with the life sciences, in the context of laboratories. It also discusses the environment and communities connected to those laboratories. The article notes that technology use is increasing, and this is true for individuals in our society, as well as for those in various governments, organizations, and for the economies of numerous nations. Many parts of our lives are affected by technology. However, we are not adequately prepared for managing security challenges associated with the use of that technology. This article identifies cybersecurity threats to life sciences laboratories, and discusses ways that these threats may be handled. Refreshingly, this article also mentions the cyber-related benefits expected to be a part of future laboratories. This article takes a practical approach to the subject of protecting the cybersecurity of laboratories, and suggests an approach that puts deliberate thought and consideration into all parts of the laboratory.

Article:

Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J., Schiel, J., Baker, J. C., Strychalski, E.A., Rogers, K. C., & Lee, K. H. (2019). Cyberbiosecurity for biopharmaceutical products. *Frontiers in Bioengineering and Biotechnology*, *7*, 116.

Link to this article:

https://www.frontiersin.org/articles/10.3389/fbioe.2019.00116/full

Key words/potential industry:

cyberbiosecurity, biopharmaceutical, manufacturing, product, medical, science, biotechnology

Article summary:

This article concerns the cyberbiosecurity threats that can occur in biopharmaceutical manufacturing. It begins with a good description of what cyberbiosecurity means. Cyberbiosecurity threats can occur where biotechnology and the cyber world meet. As we use

more technology in the biopharmaceutical sciences, we must also take precautions that the technology used is properly protected from threats. Vulnerabilities can exist in the cyber world as it connects to the biopharmaceutical manufacturing process, and vulnerabilities can even be present in the biopharmaceutical products. Cyberbiosecurity is becoming more and more important in the United States as we increase our technology use in the biopharmaceutical field. This article discusses current cyberbiosecurity vulnerabilities in the biopharmaceutical field, which can include those threats that occur along the supply chain. The article highlights threats to the biopharmaceutical manufacturing enterprise, and discusses ways to potentially handle those threats.

Article:

NCC Group (n.d.). Cyber security in U.K. agriculture [PDF]. Retrieved from https://www.nccgroup.com/globalassets/our-research/uk/images/agriculture-whitepaper-final-online.pdf

Link to this article:

https://www.nccgroup.com/globalassets/our-research/uk/images/agriculture-whitepaper-final-online.pdf

Key words/potential industry:

cybersecurity, UK, agriculture, food, network, system, life, science

Article summary:

This is a whitepaper that discusses cybersecurity in UK agriculture. It also addresses cybersecurity implications for the food system. It makes connections among agriculture, the food system, and threats that can occur on a global level. The food system is not considered vulnerable to threats severe enough to cause catastrophic effects on the level of seriously threatening food availability. This is because our food system has the ability to recover from disruptions to its functioning. However, it is possible for cybersecurity threats to cause financial losses to agricultural industries. Because the food system is connected with other parts of the economy, it is also possible for cyberattacks to the food system to affect other industries, and

infrastructure. This paper suggests that public perception can affect how bad a threat can become. This paper raises issues including data privacy, threat awareness, and the use of new technology.

Article:

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agricultural industry. *International Food and Agribusiness Management Review*, *21*(1030-2018-1811), 317-334.

Link to this article:

https://www.wageningenacademic.com/doi/pdf/10.22434/IFAMR2017.0045

Key words/potential industry:

Cybersecurity, cyberbiosecurity, cyberattack, farm, agriculture, industry, U.S., survey, technology

Article summary:

This study's methods involve a cybersecurity survey of people in the field of agriculture. Respondents included agribusiness owners and farmers. Constructs measured included severity, perception of susceptibility, self-efficacy, barriers, benefits, and prompts to action. Interestingly, this study investigated whether the farmers and agribusiness owners were previously subjects of cyberattack, and what technology was implemented. The study found that a person's decision to use secure technology was linked to perceptions of susceptibility to cyberattack and perceptions of benefits related to such protective technology. This study informs us about how people in agriculture react to security threats. Over fifty percent of those who responded to the survey had in some way been victims of cyberattack in the form of a computer security issue. The information from this study also helps us to understand what causes people to adopt measures towards preventing cyberattacks.

Article:

2018 Public-Private Exchange Program (2018). Threats to precision agriculture [PDF]. Retrieved from https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Link to this article:
https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Key words/potential industry:
precision, agriculture, threats, vulnerability, data, food, crop, livestock, production

Article summary:

This paper discusses threats to security related to technology use in agriculture. This includes technology used in both livestock production and in farming crops. Farms that use precision agriculture benefit from the use of this technology, whether it be in the form of GPS, sensors, agricultural communications, or other technology uses. Precision agriculture technology can lead to increased yields with lower costs. But those in the agricultural industry must be aware of the potential dangers associated with technology use. The increased use of technology in agriculture raises the potential for cyber related attacks. Threats identified in this paper are broadly defined as those involving attacks on integrity, availability, and confidentiality of needed inputs. The paper delves deeper into each threat type using some thought provoking and illustrative scenarios. Finally, this paper discusses potential practices for reducing cyber-related vulnerabilities in precision agriculture.

Article:
Vota, W. (2020). Lessons learned measuring, evaluating, and learning with big data. Retrieved from https://www.ictworks.org/lessons-learned-measuring-evaluating-and-learning-with-big-data/#.XwkYkR17nYJ

Link to this article:

https://www.ictworks.org/lessons-learned-measuring-evaluating-and-learning-with-big-data/#.XwkYkR17nYJ

Key words/potential industry:

big, technology, evaluation, complex, cybersecurity, data, science, organization, policy

Article summary:

This article discusses big data in the context of evaluation. It serves as a good example of how a specific field is affected by increased use of technology, and it raises several big data-related considerations. This article discusses the many benefits that the use of big data has brought to the field of evaluation, such as quick access to data, and the availability of greater sample sizes. However, it also notes that the world of big data is unfamiliar and complex to us. The article specifically mentions that big data is subject to privacy invasions, security threats, and the potential for fraud. Integration of evaluation and data science require data and technical access, and backing from policies and organizational structures. Challenges include access barriers, privacy issues, bias, and other issues. Finally, this article provides recommendations on how to make integration of evaluation and data science work well.

Article:

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer*, *52*(3), 58-66.

Link to this article:

https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1290&context=usma_research_papers

Key words/potential industry:

cyberbiosecurity, multidisciplinary, curriculum, education, academia, military, business

Article summary:

This article suggests that there are aspects of cybersecurity that are both multidisciplinary and interdisciplinary. The field is multidisciplinary in team contexts, and interdisciplinary in individual contexts. There is not a sole cybersecurity curriculum that may be used to teach about cybersecurity. Aspects of many disciplines need to be involved in building a curriculum that produces an educated cybersecurity team. Experts from several disciplines are needed in order to create successful approaches that can counter the unpredictable nature of cybersecurity threats. These experts must function in teams to help inform the process to determine both risks and solutions. This article suggests that using multidisciplinary teams allows us to take a more holistic approach to cybersecurity, considering the evolving, adaptive nature of cybersecurity threats. The future of this research is in further developing its multidisciplinary side so that experts in many fields can be involved in tackling cybersecurity challenges.

Article:

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework.

Link to this article:

https://csrc.nist.gov/publications/detail/sp/800-181/final

(this link takes you to the document abstract, and you can click on the article on the right side of the page).

Key words/potential industry:

cybersecurity, national, framework, workforce, development, education, government, academia, private

Article summary:

This is a lengthy resource that details the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework). This publication emphasizes that cybersecurity is interdisciplinary. This is a helpful resource for anyone interested in engaging in improving organizational cybersecurity. This resource is also useful for those who

wish to tailor an organization's cybersecurity approach to the organization itself. It includes an Executive Summary that can assist those who wish to review a brief synopsis of the publication's cybersecurity-related and workforce development-related content without reading the document in its entirety. The publication describes the use of a cybersecurity workforce for handling the cybersecurity issues an organization may face. The document may be used to help an organization to communicate about cybersecurity. It is of assistance to organizations interested in developing their own publications or resources about cybersecurity, and presents a framework that may be used to shape organizational initiatives.

Article:

USDA (2020). USDA-NIFA and NSF establish nationwide network of artificial intelligence research institutes.

Link to this article:

https://nifa.usda.gov/press-release/artificial-intelligence-research

Key words/potential industry:

National, nationwide, network, artificial, intelligence, research, institute, USDA, NIFA, NSF

Article summary:

This article describes a nationwide network of institutes for artificial intelligence research. There are to be seven artificial intelligence institutes for research. Five of these are NSF AI institutes, and two are USDA-NIFA AI institutes. This represents a very large investment in artificial intelligence research on the federal level. These institutes are to focus not just on research, but also on the U.S. workforce, and the needs of the future. These institutes are very important because research on artificial intelligence is expected to have positive implications for aspects of the economy, as well as safety and health. These institutes involve the U.S. Department of Transportation, the U.S public research universities, and the research and development arm of the U.S. Department of Homeland Security. The seven research institutes are expected to be informational hubs to help in critical spheres such as severe weather preparation, education, workforce development, and agriculture.

Article:

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.

Link to this article:

https://www.ehidc.org/sites/default/files/resources/files/Ed_You_Testimony_USCC.pdf

Key words/potential industry:

Bioeconomy, U.S., China, security, biotechnology, biological, government

Article summary:

This document is the March 16, 2017 testimony of Edward You for the U.S.-China Economic and Security Review Commission. Edward You is identified in the document as Supervisory Special Agent, Biological Countermeasures Unit, Countermeasures and Operations Section, Weapons of Mass Destruction Directorate, Federal Bureau of Investigation. The testimony details issues surrounding the bioeconomy of China and the United States. It describes ways that the United States can handle biological threats, and security issues the United States faces. Changing the United States's focus towards new biotechnologies can help it widen the scope of what is considered a biological threat, and help the United States to better prepare for these potential threats. This testimony also describes how additional developments in industry, and research in biotechnology, can help boost national security. Informal recommendations include coupling security measures with innovation, and expanding the understanding of the bioeconomy towards closing gaps in risk assessment.

Article:

Kozminski, K. G. & Drubin, D. G. (2015). Biosecurity in the age of Big Data: A conversation with the FBI. *Molecular Biology of the Cell*, *26* (22), 3894-3897.

Link to this article:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4710219/

Key words/potential industry:

Biosecurity, FBI, big, data, science, technology, security, life science

Article summary:

This article details a discussion with Edward You, Supervisory Special Agent, Biological Countermeasures Unit, Countermeasures and Operations Section, Weapons of Mass Destruction Directorate, Federal Bureau of Investigation. The discussion centers on biosecurity and Big Data, and it bridges the gap between national security and the life sciences. The discussion mentions that a priority is to prevent another 9/11 from occurring. It can be challenging to support both national security and the life sciences at once. The FBI keeps an eye out for ways to protect the life sciences, and takes a proactive approach in that respect. Big Data is considered to be a step in the evolution of the emerging areas that must be proactively identified to properly prepare for potential threats. Personalized medicine is an example of an area that is very data dependent. Overall, partnerships between the sciences and the FBI are critical for security awareness.

Article:

Pauwels, E and Dunlap, G. (2017). The intelligent and connected bio-labs of the future: The promise and peril in the fourth industrial revolution [PDF file]. Washington, DC: The Wilson Center.

Link to this article:

https://www.wilsoncenter.org/sites/default/files/media/documents/publication/dunlap_pauwels_intelligent_connected_biolabs_of_future.pdf

Key words/potential industry:

Biological, lab, intelligence, intelligent, industry, technology

Article summary:

The way that research is conducted is affected by the fast speeds in which technologies continue to develop. The speed of technological advancement affects not only the way that research is conducted, but also who is involved in conducting the research. This article gives several good examples of ways that technology has advanced towards increasing the connectivity of the modern laboratory. It also describes how laboratories have become more intelligent. Examples of the ways that laboratories have become more intelligent include increased automation, as well as the ability to perform laboratory functions remotely. While this use of technology in the laboratory is helpful for researchers, the technology used in the intelligent laboratory can also be subject to exploitation from malicious parties. Because technology is advancing so quickly, it is challenging to keep up with the pace at which threats may present themselves, but technology-based defenses are available.

Article:

Pauwels, E. and Vidyarthi, A. (2017). Who Will Own the Secrets in Our Genes? A U.S. – China race in artificial intelligence and genomics [PDF file]. Washington, DC: The Wilson Center.

Link to this article:

https://www.scribd.com/document/339612675/Who-Will-Own-the-Secrets-in-Our-Genes

Key words/potential industry:

Gene, medicine, precision, U.S., China, AI, genomics, biosecurity

Article summary:

This article discusses international competition in genomics and precision medicine. It specifically discusses competition between the U.S. and China. The article notes that China has made heavy investments in the combination of gene-related technology and artificial intelligence. This combination has the ability to advance our understanding of medicine, and can help to show us new directions and insights in precision medicine. The U.S. needs to plan for future competition on this front from China. The dynamics of the relationship that the U.S. and China will maintain in regard to precision medicine may depend on our own policies, including science policy, as well as our own diplomatic efforts. Biosecurity, including the protection and

management of data, is at issue in this situation. This article raises many questions about the future of U.S.-China relations in regard to biosecurity, genomics, research, and technology.

Article:

Pauwels, E. and Vidyarthi, A. (2016). How our unhealthy cybersecurity infrastructure is hurting biotechnology [PDF file]. Washington, DC: The Wilson Center.

Link to this article:

https://www.scribd.com/document/306290051/How-Our-Unhealthy-Cybersecurity-Infrastructure-is-Hurting-Biotechnology

Key words/potential industry:

Biotechnology, cybersecurity, healthcare, government, biotechnology, data, security

Article summary:

Data security is of great importance for those involved in handling sensitive data. This is especially true for the health care industry, which frequently manages personal data as a matter of course. There have been security breaches recently that have caused the health care industry, as well as governments, to look harder at the issue of cybersecurity. The biotechnology sector has been growing at a faster pace than the economy itself. Policy surrounding cybersecurity does not always center on the biotechnology sector. The combination of the growth in the biotechnology sector and the fact that policy is not keeping pace with its growth poses a challenge. This challenge can serve as a threat to both the life sciences, and business. Data can be threatened by modification, theft, and the potential for its use in other malicious ways. Priority must be given to data security.

Article:

National Academies of Sciences, Engineering, and Medicine. 2020. *Safeguarding the Bioeconomy*. Washington, DC: The National Academies Press.

Link to this article:

https://www.nap.edu/catalog/25525/safeguarding-the-bioeconomy

Key words/potential industry:

Bioeconomy, U.S., leadership, government, research, threats, STEM, cybersecurity

Article summary:

Innovation is helping fields within the life sciences to grow. The economic activity associated with these fields within the U.S. economy is our bioeconomy. A common definition of bioeconomy is needed to accurately assess the breadth of the bioeconomy. This definition must include current and future developments. Numerous factors, including definitions, make it difficult to analyze the contributions to, and value of, the bioeconomy to the country's economy. It is agreed to be extensive, and must be safeguarded to allow for continued support and growth. To do this, leadership will need to be established to coordinate and oversee the collaboration of the many fields which contribute to the bioeconomy, including training and retaining a skilled technical workforce. Collaboration is needed to create an open scientific environment while protecting the economy from exploitation from other countries. This collaboration creates cybersecurity concerns which must be managed for successful information sharing and research.

Article:

Zhou, J., Reynolds, D., Le Cornu, T., Websdale, D., Orford, S., Lister, C., Gonzalez-Navarro, O., Laycock, S., Finlayson, G., Stitt, T., Clark, M. D., Bevan, M. W., Griffiths, S. (2017). CropQuant: An automated and scalable field phenotyping platform for crop monitoring and trait measurements to facilitate breeding and digital agriculture. *BioRxiv*.

Link to this article:

https://www.biorxiv.org/content/10.1101/161547v2

Key words/potential industry:

phenotyping, technology, crop, research, CropQuant

Article summary:

This article presents a cost-effective and easy field phenotyping platform called CropQuant. Phenotyping technologies are vital to crop research as they provide precise and continuous measures of traits. Such measurements are very important for agricultural research. These trait measurements assist with crop production and breeding. The CropQuant platform is both scalable and automated, allowing for use in various places, rather than being restricted in use to just one type of environment. Realtime interactions were made possible by CropMonitor, a web-based system developed to manage experiments in the field. It allows for collection of crop-climate data, and has a helpful graphical interface. This interface is called the graphical user interface, or GUI. Actions among environmental factors, phenotypes, and genotypes were studied on CropQuant workstations. This article reports the results of the use of these technologies in previous field experiments, including in trait analyses.

Article:

Durrell, K. (2019). The buzz around insect protein: Protix inaugurates €45 million facility in the Netherlands. *Food Ingredients First*.

Link to this article:

https://www.foodingredientsfirst.com/news/the-buzz-around-insect-protein-protix-inaugurates-%E2%82%AC45-million-facility-in-the-netherlands.html

Key words/potential industry:

insect, protein, Netherlands, sustainability, Protix, alternative

Article summary:

This article is about the production of insect protein for animal consumption, such as for salmon and chicken feed. The largest insect processing plant, producing protein for animal nutrition, opened in the Netherlands in June of 2019. The use of insects as an alternative protein source is a growing industry. With this new facility, Protix has proof of successful industrial scale insect protein production, utilizing technology through their automated process, and resulting in improvements in consistency and quality. Insect are well-suited to help increase sustainability in the food industry while reducing waste. Requirements for space and fertile land are limited, decreasing insects' carbon footprint and increasing their appeal as a protein source for animals. Protein sourced from insects may also lead to benefits for the animals consuming the protein. With consumers looking for brands which invest in sustainability, further growth of insect protein companies can be anticipated.

Article:

Chabrow, E. (2011). Creating Ag Extension Agent for Cyber: Championing a new way to spread infosec awareness. *Gov Info Security*.

Link to this article:

https://www.govinfosecurity.com/interviews.php?interviewID=1216

Key words/potential industry:

Cybersecurity, legislation, extension, U.S. government

Article summary:

Businesses and individuals are forced to operate in an online environment that is not safe due to inconsistently protected systems. Legislation is being drafted to set reporting and protection standards for information. This legislation would supersede some current state laws.

USACM created a list of privacy principles they would like to see in legislation and which are currently not present. Committees in Congress cause difficultly in properly creating and passing cybersecurity legislation due to the overlapping categories cybersecurity falls into. Bills must go to the appropriate committee, but cybersecurity bills are fragmented, separated into multiple committees, each fighting for jurisdiction, and resulting in little progress. Furthermore, cybersecurity education and assistance are currently lacking. Utilizing the current ag extension model for cybersecurity could be of great benefit providing somewhat local and accessible guidance on prevention and response to privacy breaches or issues.

Article:

The White House. (2012). *National Bioeconomy Blueprint*. Washington. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf

Link to this article:

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf

Key words/potential industry:

Bioeconomy, U.S., future, research, development, education, training, regulations

Article summary:

The bioeconomy has recently become a priority due to its potential for growth, and the overall benefits it brings to our society. The bioeconomy growth in the U.S. is because of developments in technology, such as DNA sequencing and genetic engineering. Along with this focus and development comes ethical, safety, and security concerns. The National Bioeconomy Blueprint was created in 2012 to layout objectives and highlight achievement. The first objective

focuses on R&D investment that is both coordinated and integrated. The second includes committing to proper and efficient transition of technologies and inventions from the lab to the market. The third objective discusses implementing and adapting new and current regulations to protect human health and the environment. The fourth objective shifts to focus on training programs and proper education. Finally, the fifth objective looks towards development of partnerships and collaboration to benefit the broader bioeconomy.

Article:

Mulvany, L. (2019). Deere Outlook Disappoints as Trade War Keeps Farmers Frugal. *Bloomberg.*

Link to this article:

https://www.bloomberg.com/news/articles/2019-11-27/deere-fourth-quarter-net-sales-beat-highest-estimate

Key words/potential industry:

Deere & Co., U.S., China, trade, shares, sales, agriculture

Article summary:

In 2019, trade tensions between the U.S. and China have made Deere & Co. take a cautious outlook on the future. This article describes North American farmers avoiding buying large equipment, leaving demand for these machines low, and causing Deere & Co. shares to drop to a six-week low. The article describes the CEO as expecting a conservative net income projection. It mentions that the forecast for global sales of agriculture and turf equipment are set to fall up to 10% while construction and forestry equipment are set to see closer to 15%. At the time of the article's writing, government payments were expected to reach farmers in time to

increase demand for Deere for the second quarter. Additionally, the article mentions that a U.S.-China trade deal could have the effect of potentially helping to provide a boost to agriculture in North America.

Article:

Daniels, K. (2020). Researchers apply new technology to identify plant pathogen strains in Virginia. *Virginia Tech Daily*.

Link to this article:

https://vtnews.vt.edu/articles/2020/01/FLSI-vinatzer-plant-pathogen-technology.html

Key words/potential industry:

Plant, disease, research, technology, pathogens, Virginia Tech

Article summary:

A team of scientists at Virginia Tech have been successful in identifying plant pathogens down to the strain using Oxford Nanopore Sequencing MinION along with bioinformatic programs and sequencing databases. Identification to the specification of strain can be extremely challenging, but is important to ensure the proper response measures are taken for the proper strain. Misidentification of the specific strain causing plant health problems can result in untreated diseases. New technology allows for one test to be completed to identify the pathogen whereas in the past a separate test would be needed for each possible pathogen, taking time and resources. LINbase was created by Vinatzer and Heath to be a comprehensive database focused on plant pathogens since, prior to this, one did not exist. The lab hopes to share their findings and processes to improve plant disease diagnostics to all levels of growers.

Article:

Corteva Agriscience (2020, April 29). *MercyOne and Corteva Agriscience Join Forces to Increase COVID-19 Sample Testing*.

Link to this article:

https://www.corteva.com/resources/media-center/mercyone-and-corteva-join-forces-to-increase-covid-19-sample-testing.html

Key words/potential industry:

COIVD-19, testing, healthcare, MercyOne, Corteva Agriscience

Article summary:

MercyOne, a system of healthcare facilities with headquarters in central Iowa, partnered with Corteva Agriscience, a global agriculture company, to process COVID-19 samples. This collaboration is expected to assist with the urgent processing of these samples. This collaboration helps in adding to our overall potential to achieve COVID-19 test results more quickly. The initial focus will be in Iowa to fill a need for processing ability of these samples in that region. Testing is planned to continue as long as is needed but Corteva Agriscience facilities do not have plans to assist with sample collection. The collaboration involves two steps. First, health care workers with MercyOne collect the samples involved in the processing. Then, employees of Corteva process the samples. This is considered an innovative collaboration between MercyOne and Corteva Agriscience, and it is designed to better meet the needs of the community.

Article:

Bedord, L. (2016, April 5). Midwest Agriculture Is A Prime Target For Theft Of Intellectual Property And Cyber Attacks. *Successful Farming*.

Link to this article:

https://www.agriculture.com/content/cybersecurity-is-not-just-a-big-city-problem

Key words/potential industry:

Midwest, agriculture, cybersecurity, intellectual property, cyber-attack, biotechnology, technology, security, terrorism

Article summary:

Trade secrets and intellectual property are at risk of attack from inside and outside companies, and the attack can come from inside or outside the country. With agriculture on the rise, in part due to biotechnology, companies are at an increasing risk of cyber-attacks. When a company produces a valuable product, a competitor may want to have that same product. This makes midwestern agriculture a target of threats. Biotechnology as produced high yield crops with the help of sensors, drones, satellites, and other technologies. Though the innovation is beneficial to the sector, it is also resulting in security threats. Farmers utilizing new technologies are at risk for being hacked, as some already have, with no plan for what to do when it occurs. Businesses of all sizes should have a plan in place, but many do not, leaving them at further risk of cyber-attack or terrorism in agriculture.

Article:

Gaffney, J., Schussler, J., Loffler, C., Cai, W., Paszkiewicz, S., Messina, C., Groeteke, J., Keaschall, J., Cooper, M. (2015). Industry-Scale Evaluation of Maize Hybrids Selected for Increased Yield in Drought-Stress Conditions of the US Corn Belt. *Crop Science, 55*(4).

Link to this article:

https://acsess.onlinelibrary.wiley.com/doi/full/10.2135/cropsci2014.09.0654

Key words/potential industry:

Maize, hybrids, drought, US Corn Belt, agriculture, food security, crop yield

Article summary:

This article describes research designed to improve maize crop resilience to drought conditions. Historically common droughts are one of many challenges facing agricultural production. Fields do not always receive the natural rainfall the plants need in order to yield an optimal crop. Proper water is especially important in critical stages of plant development, such as flowering. Intensive breeding and agronomic practice improvements have resulted in an increase of hybrid maize production. Improved yield coupled with best management practices to conserve soil and water are needed. AQUAmax hybrid maize has been shown to provide increased yield despite drought while providing slightly above normal yield under favorable conditions when compared to non-AQUAmax hybrids. After three years of research followed by three years of on the farm testing, AQUAmax hybrids were shown to offer yield stability for farmers when the plants were produced under each water-limited conditions and favorable growing conditions.

Article:

iGrow (2016). *AeroFarms Plans Largest Indoor Vertical Farm of Its Kind.*

Link to this article:

https://www.igrow.news/igrownews/aerofarms-plans-largest-indoor-vertical-farm-of-its-kind

Key words/potential industry:

Agriculture, agribusiness, innovation, farming, technology, vertical, farm, AeroFarms

Article summary:

Year-round local commercial production of leafy greens has been made possible by AeroFarms's innovative growing technology, which uses less space and water while being pesticide, fungicide, and herbicide free. Headquartered in Newark, New Jersey, the company

announced its first Virginia site to be in the City of Danville and Pittsylvania County. Virginia and North Carolina each wanted to have this project within their state, and Virginia was successful in outcompeting North Carolina. As AeroFarms's name suggests, it grows plants aeroponically. The new indoor farm will increase the area's access to year-round healthy foods while providing jobs and growth for the area. The new location will be the largest indoor vertical farm like it, at almost double the size of the company's last New Jersey facility. With Virginia's already strong agricultural industry, the Commonwealth is looking forward to expanding its agricultural technology and continuing to advance its food system.

Article:

FDA. (2020, July 30). 2020 Leafy Greens STEC Action Plan. Retrieved from https://www.fda.gov/food/foodborne-pathogens/2020-leafy-greens-stec-action-plan

Link to this article:

https://www.fda.gov/food/foodborne-pathogens/2020-leafy-greens-stec-action-plan

Key words/potential industry:

food safety, outbreak, foodborne illness, STEC

Article summary:

Though leafy greens are important for a healthy diet and are commonly and widely consumed, foodborne outbreaks are often traced back to this product. Specifically, outbreaks of Shiga toxin-producing E. coli, which can cause life-threatening foodborne illness for some, have been linked to leafy greens. As many leafy greens are consumed without heat processing to reduce or eliminate microbes which can be introduced during the growing and processing of the product, the FDA has recognized that the safety of the greens we produce needs to be prioritized

to reduce outbreaks and increase consumer safety. In response to concerns about foodborne illness from consumption of leafy greens, FDA has outlined the planned actions scheduled for 2020, with focus in areas of prevention, addressing gaps in knowledge, and response. These steps will require urgent collaboration focused on actions among FDA, stakeholders, industry, and regulatory groups.

Article:

Engelking, C. (2019, March 19). Edible Insects Are The New Animal Farm. *Discover Magazine*.

Link to this article:

https://www.discovermagazine.com/planet-earth/edible-insects-are-the-new-animal-farm

Key words/potential industry:

Farm, insects, agriculture, innovation

Article summary:

The cricket life cycle has been optimized in a commercial cricket farm in Austin, Texas where around one million crickets are raised daily for human consumption. An operation this size for human use had never been done before Aspire Food Group launched their farm. Edible insects are much less demanding on farmers and valuable resources when compared to the livestock industry. With an increasing population around the globe, insects could be an important contributor in solving the world hunger issue. The industry sector is expected to continue to grow over the next few years as multiple companies attempt to enter the industry with their own cricket farms and products. The industry is hoping to convince consumers, especially in the U.S. and Europe, who are currently opposed to insect consumption, that crickets and cricket products can be a high protein option worth integrating into their diet.

Article:

Upson, L. (2016, October 6). Introducing the Debug Project [Blog post].

Link to this article:

https://blog.verily.com/2016/10/introducing-debug-project.html

Key words/potential industry:

Insects, disease, technology, biology, mosquitoes, sterile insect technique

Article summary:

Millions of people are sickened by disease spread by mosquitoes each year. The sterile insect technique (SIT) has emerged as a method to combat the spread of disease by mosquito. SIT involves releasing sterile insects so they will mate with wild insects. These matings do not produce offspring, thus reducing the wild population, and possibly resulting in elimination of the wild population on a local level. The SIT was first developed in response to New World screwworm and is currently used to control Mediterranean fruit flies. SIT has been attempted to control mosquitoes before, but radiation to sterilize them caused further complications with mating abilities. New techniques created to sterilize the mosquitoes have eliminated this problem. Additionally, only male mosquitoes need to be released as they do not feed on blood, however, separating males and females is costly and labor intensive. Automation will be the focus of reducing costs.

Article:

Bipartisan Commission on Biodefense. (2015). *A national blueprint for biodefense: Leadership and major reform needed to optimize efforts – Report of the Bipartisan Commission on Biodefense*. Washington, DC: Hudson Institute.

Link to this article:

https://biodefensecommission.org/reports/a-national-blueprint-for-biodefense/

Key words/potential industry:

biodefense, U.S., biological crisis, bioterrorism, biosurveillance, government

Article summary:

A national blueprint could guide the United States to large improvements in the nation's biodefense. While many types of threats receive special attention and leadership, biological threats do not always have the same level of focus. This document mentions a lack of a central individual leading biodefense. The Vice President can lead biodefense with a budget dedicated to biodefense. Control, coordination, prioritization, and accountability would stem from leadership to work towards proper defense against biological threats across multi-disciplinary efforts. Lack of coordination at high levels negatively impacts lower levels, which require proper integration along with proper funding and strategy. Along with the federal function should come local biodefense capabilities to be aided by the federal government. These should include investments in biosurveillance systems, health systems, and emergency services. Proper leadership could drastically improve the nation’s preparation and response to biological threats.

Article:

Bipartisan Commission on Biodefense. (2017). *Special focus: Defense of animal agriculture*. Washington, DC: Bipartisan Commission on Biodefense.

Link to this article:

https://biodefensecommission.org/reports/defense-of-animal-agriculture/

Key words/potential industry:

agrodefense, zoonotic, disease, infectious, outbreak, government, U.S., agriculture, biodefense, security

Article summary:

The Food and Agriculture sector is one of the largest in the U.S. economy. With new and recurring zoonotic diseases and threats to food systems continuing, vulnerabilities must be mitigated or eliminated. These concerns are of national security due to their high importance. Animals and plants needed for products such as foods and fibers are critical to the biodefense mission, which is extremely complex. Leadership of this mission should be centralized, and headed by the Vice President with appropriate extensions of expertise. Increased collaboration is necessary between the USDA and FBI to better respond to outbreaks due to natural events or purposeful action. Additional collaboration is needed for detection and surveillance of disease in livestock production as well as in wildlife. Protecting agriculture is very important for creating the products that we need. As current response plans are insufficient, innovation will be required for the necessary improvements.

Additional Resources

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* [PDF file]. Retrieved from https://www.aaas.org/sites/default/files/AAAS-FBI-UNICRI_Big_Data_Report_111014.pdf

Consumer Story: Aero Farms. *Dell Technologies*. Retrieved from https://www.delltechnologies.com/nl-be/case-studies-customer-stories/aerofarms.htm#collapse=0

Bipartisan Commission On Biodefense. (2020, September 24). The Biological Event Horizon: No Return or Resilience [Video file]. Retrieved from https://www.youtube.com/watch?v=N-1oUAhJIMU&feature=emb_title

Commonwealth Cyber Initiative (n.d.). *Research with impact*. https://cyberinitiative.org/

Ferrag, A. M., Shu, L., Yang, X., Derhab, A., Maglaras, L. (2020). Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. IEEE Access, 8, 32031 – 32053. Retrieved from https://ieeexplore.ieee.org/document/8993722

Fischer, D. (2014, May 30). Monsanto Suffers Data Breach at Precision Planting Unit. *Threat Post*. Retrieved from https://threatpost.com/monsanto-suffers-data-breach-at-precision-planting-unit/106378/

Hvistendahl, M. (2020). *The Scientist and the Spy: A True Story of China, the FBI, and Industrial Espionage*. Riverhead Books.

Murch, R. (2019, May 1). Security Vulnerabilities in the Bioeconomy Existed Prior to Synthetic Biology [PDF PowerPoint Slides]. Retrieved from https://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_192712.pdf

National Academies of Sciences, Engineering and Medicine (2015). *Safeguarding the Bioeconomy II: Applications and Implications of Emerging Science* [PDF file]. Retrieved from https://www.ehidc.org/sites/default/files/resources/files/Safeguarding%20the%20Bioeconomy_II_Recap%20Final%20090815.pdf

National Academies of Sciences, Engineering and Medicine (2016). *Safeguarding the Bioeconomy III: Securing Life Sciences Data* [PDF file]. Retrieved from https://www.ehidc.org/sites/default/files/resources/files/Safeguarding_the_Bioeconomy_III_Recap.pdf

National Institute of Standards and Technology (n.d.). *Cybersecurity framework*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology (n.d.). *National Institute for Cybersecurity Education (NICE)*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology (n.d.). *NICE framework resource center*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

National Institute of Standards and Technology (n.d.). *Privacy framework*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology (n.d.). *Workforce advancement.* https://www.nist.gov/cyberframework

National Research Council (U.S.). Committee on a New Biology for the 21st Century: Ensuring the United States Leads the Coming Biology Revolution, & National Research Council (U.S.). (2009). *A new biology for the 21st century*. National Academies Press.

Newman, L. H. (2020, July 27). A Cyberattack on Garmin Disrupted More Than Workouts. *Wired*. Retrieved from https://www.wired.com/story/garmin-outage-ransomware-attack-workouts-aviation/

Reisch, M. S. (2011, September 26). Scientists Admit to Trade Secret Theft. Chemical and Engineering News, 86(39). Retrieved from https://cen.acs.org/articles/89/i39/Scientists-Admit-Trade-Secret-Theft.html

Riley, D. (2020, September 24). DHS discloses data breach of US agency but doesn't name which was hacked. *Silicon Angle*. Retrieved from https://siliconangle.com/2020/09/24/dhs-discloses-data-breach-us-agency-doesnt-name-hacked/

The Roanoke Star (2020, June 1). *Commonwealth cyber initiative awards learning grants to faculty and students across Virginia*. The Roanoke Star. https://theroanokestar.com/2020/06/01/commonwealth-cyber-initiative-awards-learning-grants-to-faculty-and-students-across-virginia/

Shoup, M. E. (2020, September 25). Revol Greens closes $68m funding round to become 'world's largest indoor lettuce producer'. *Food Navigator-USA*. Retrieved from https://www.foodnavigator-usa.com/Article/2020/09/25/Revol-Greens-closes-68m-funding-round-to-become-world-s-largest-indoor-lettuce-producer

Siler, J., Goldberg, L., Rona, A. (Producers), & Collet-Serra, J. (Director). (2011). Unknown [Motion picture]. United States: Warner.

Stwart, J., Richards, J. Cyber Security: Staying safe while surfing the web. UT Extension Institute of Agriculture [PDF file]. Retrieved from https://extension.tennessee.edu/publications/Documents/W539.pdf

United States, Congress, Office of Technology Assessment. Technology Assessment and the Work of Congress. Congress of the U.S., Office of Technology Assessment. Retrieved from https://www.princeton.edu/~ota/ns20/cong_f.html

United States, Congress, Office of Technology Assessment. (1992). *A new technological era for American agriculture*. Congress of the U.S., Office of Technology Assessment.

University of California. (2000). California Agriculture 2000 (Vol. 54, 4). On the horizon: Agriculture's new millennium.

United States Department of Agriculture (2020, July). *Agriculture and food research initiative-foundational and applied research program*. https://nifa.usda.gov/funding-opportunity/agriculture-and-food-research-initiative-foundational-applied-science-program

U.S. Department of Health and Human Services Office for Civil Rights (n.d.). *Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information.* U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

US Department of Homeland Security CSIA Cyber and infrastructure. (2020). Analysis Report (AR20-268A). Retrieved from https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a

4-H Code Camp. (2021). WV Extension Service. Retrieved from https://extension.wvu.edu/youth-family/4h/events/code-camp

U.S. Department of Health and Human Services Office for Civil Rights (n.d.). *Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information*. U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Other Resources of Interest

Precision planting, is this precision ag? Dennis Fisher (May 30, 2014) Online article.
Convergence: Safeguarding Technology in the Bioeconomy (2014).
Monsanto files lawsuit over stolen computer data. Chemical & Engineering News.
United States Department of Agriculture. *Search for a funding opportunity*. https://www.nifa.usda.gov/page/search-grant