Safeguarding the Bioeconomy: Applications and Implications of Emerging Science

Meeting Recap

July 27-28, 2015

The National Academies of Sciences, Engineering, and Medicine conducted a workshop to assist the Federal Bureau of Investigation Weapons of Mass Destruction Directorate in understanding the applications and implications of emerging technologies at the interface of the life sciences, chemical sciences, and other areas of science and engineering. Workshop participants identified and discussed areas of convergence in the life sciences research enterprise, how these emerging areas may be incorporated into the global bioeconomy, and the security implications of their development.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Board on Chemical Sciences and Technology

Meeting Recap

Safeguarding the Bioeconomy: Applications and Implications of Emerging Science

July 27-28, 2015

Disclaimer: This meeting recap was prepared by staff of the National Academies of Sciences, Engineering, and Medicine ("Academies") as an informal record of issues that were discussed during public sessions of the Academies' Workshop on Safeguarding the Bioeconomy: Applications and Implications for Emerging Science, held on July 27 and 28, 2015. This document was prepared for information purposes only and as a supplement to the meeting agenda. It has not been reviewed and should not be cited or quoted, as the views expressed do not necessarily reflect the views of the Academies or the Committee on Safeguarding the Bioeconomy: Applications and Implications of Emerging Science.

INTRODUCTION

DEFINING THE BIOECONOMY

The White House and the Office of Science and Technology Policy define a bioeconomy as "*one based on the use of research and innovation in the biological sciences to create economic activity and public benefit" including "economic activity that is fueled by research and innovation in the biological sciences*."[1] Working within this definition, the U.S. bioeconomy is both vast and penetrating. Sectors of the bioeconomy span healthcare and medicine, pharmaceuticals, biotechnology, informatics, and agriculture. Together, these sectors comprise up to $4 Trillion or 25% of the U.S. GDP.[2] Over the decades, biological research and innovation in the biological sciences and technology have yielded immense advances in these areas, contributing both to U.S. economic growth and public welfare. Direct and highly visible benefits of the flourishing U.S. bioeconomy include new pharmaceuticals and diagnostic tests in healthcare, individualized medicine, alternative energy sources and biofuels, and high-yielding agricultural crops. With its rapid growth, the U.S. bioeconomy increasingly serves as a critical foundation for American competitiveness, security, economic growth, and global leadership in research and innovation.

WORKSHOP MOTIVATION

While the continued expansion of the U.S. bioeconomy has the potential to generate significant economic and technological advancements and public benefit, it also introduces a range of complex new threats and vulnerabilities that have not been fully assessed or understood, putting at risk the significant promise of the bioeconomy for advancing vital American national interests in the 21st Century. In the past few years, it has become apparent that all informatic components of human activities are vulnerable (for example, the Snowden

[1] United States. White House Office. *National Bioeconomy Blueprint*. Washington: The White House, 2012.
[2] U.S. Bureau of Economic Analysis, 2015.

disclosures from 2013-present, the OPM data breach in 2014, and the Anthem medical record breach in 2015), and that key informatic components have already been hacked. Moreover, no individual or group currently understands the full consequences and ramifications of these developments, but these actions seem to threaten all types of economic activities that depend in any way on confidentiality, ranging from competitive innovation to criminal activities.

At the request of the Federal Bureau of Investigation (FBI), an ad hoc committee appointed by the National Academies of Sciences, Engineering, and Medicine organized a workshop of invited guests from academia, industry, non-profit, and government to exchange information and engage in discussion surrounding the applications and security implications of existing and emerging technologies within the bioeconomy. Specifically, in light of recent instances of industrial espionage and data hacks, how might stakeholders of the bioeconomy be able to recognize or identify the security vulnerabilities of existing and future technologies? Further, how are these types of attacks mitigated or prevented with the anticipation that more will occur in the future? With the rapid and continued growth of the bioeconomy, more is at stake. However, a critical balance should bet struck between preserving security, and not hampering innovation.

SESSION TOPICS

The Role of Informatics in the Bioeconomy
To facilitate how this workshop addressed the Statement of Task, workshop participants were asked to identify and discuss important bioeconomy data and bioinformatics security issues, both from a "user-driven" perspective and from a "provider and/or protector" perspective. The goals of this session were: (1) to increase awareness about the range and magnitude of threat, vulnerability, and security issues related to data and other high-value information assets that bioeconomy stakeholders are confronting; and (2) to identify changes that can increase our ability to understand and address the novel threats and vulnerabilities confronting the American bioeconomy today and in the years ahead.

Criminal Threats and Vulnerabilities in the Existing and Near-Future Bioeconomy
Participants were asked to discuss advances in biotechnology that might enable better data-gathering for known types of data as well as the generation of new data types. Workshop participants were also asked to consider how such new data might introduce new vulnerabilities to biotechnological activities and novel ways to protect them.

Securing and Flourishing the Bioeconomy for the Future
Finally, participants were asked to reconsider the previous discussions around existing and future security threats and vulnerabilities and address what is needed to expand the bioeconomy, while operating within the current context of data insecurity. Additionally, participants were asked to consider and suggest actions, strategies, and plausible modes of governance and regulation that might mitigate security threats and vulnerabilities within the U.S. bioeconomy, while simultaneously promoting its further growth and development.

MESSAGES HIGHLIGHTED DURING DISCUSSION

To inform the sponsor of existing and future security challenges and vulnerabilities within the bioeconomy, individual workshop participants presented and discussed industry-specific security issues and mitigation tactics based on their individual experiences and perspectives. These concepts and issues should not be seen as conclusions of the workshop or as consensus statements of the workshop participants or organizing committee.

The U.S. bioeconomy is large, growing, and vital to American domestic and international interests

- Sectors of the bioeconomy span healthcare and medicine, pharmaceuticals, biotechnology, informatics, and agriculture, which, if combined, equate to roughly 25% of U.S. GDP
- U.S. bioeconomy increasingly serves as a critical foundation for American competitiveness, security, economic growth, and global leadership in research and innovation

With the growth of the U.S. bioeconomy come increasing security risks and threats to physical proprietary materials and informatics

- The consequences and ramifications of these threats are currently not well understood, nor have they been assessed
- How to address these existing threats and vulnerabilities, as well as how to anticipate, mitigate, and manage those which have yet to occur

Industrial espionage and data hacks are occurring at an increasing rate

- FBI witnessed a 53% rise in the incidence of economic espionage within the past year alone
- Cases of data exfiltration are becoming more common and have already occurred with detrimental consequences (e.g. 2014 OPM data breach, 2015 Anthem medical record breach)

In an era of radical transparency, traditional security measures lose effectiveness

- Communities within the U.S. bioeconomy are increasingly operating within a context of involuntary radical transparency[3]
- In this context, formerly effective modes of security and defense, such as encryption, and lock and key mechanisms, become less applicable

Alternative and adaptable data security measures could be used while operating within the context of involuntary radical transparency

- Advanced access control and management systems could provide a more effective alternative to traditional encryption methods
- Ascribing monetary value to specific types of data, such as genomic data, could promote innovative methods of security and regulation
- Creating networks of trust and enhanced communication within the subsectors of the bioeconomy could help to identify bad actors and reduce potential harm
- Continually accelerating the rate of innovation in the bioeconomy, such that technologies become so advanced that they are insurmountable by bad actors and global competitors, could mitigate existing security risks and threats

[3] Involuntary radical transparency refers to a state of unintended data availability or openness.

Data insecurity in the bioeconomy could be considered as existing along a spectrum of risk

- The extraordinary depth of information originating from and shared within the bioeconomy is one of its most remarkable and unique characteristics, but also leaves the bioeconomy vulnerable to bad actors
- Given the uncertainty surrounding security risks in the bioeconomy, these risks might be best managed and prioritized if aligned along a temporal spectrum based on expected incidence, allowing mitigation techniques to be strategically considered and deployed at the appropriate times

Companies, organizations, and research institutions need to identify their security posture early

- All require heightened awareness and acknowledgement of existing and potential information insecurities
- Companies and other organizations would benefit from identifying and prioritizing their security posture at the levels of the board of directors and/or the chief information officer

It is critical that the U.S. maintain its global leadership and competitiveness within the bioeconomy

- Failure to maintain preeminence in research, innovation, economic competitiveness, and education and training poses a significant risk to the U.S. economy and national security
- Assuming a leadership role in raising global awareness of security issues within the bioeconomy could help bolster the U.S.'s security posture internationally and ensure its involvement in future security deliberations

Governance of the bioeconomy may be possible but with some notable parameters

- Within the bioeconomy, there exists a multiplicity of stakeholders of varying interests, and perspectives of threat and vulnerability
- Develop governance structures or regulations such that they operate within an international context
- Policies or regulations should not act as a hindrance to advancement, but instead be adaptable to continuous innovation

KEYNOTE: INDUSTRIAL ESPIONAGE – THE THEORY AND PRACTICE OF BREACHES

Dr. James Mulvenon of Defense Group Inc. (DGI) set the stage for the workshop with a keynote presentation entitled *Industrial Espionage: The Theory and Practice of Breaches*.

Rising Incidence of Industrial Espionage

There has been a stark rise in the incidence of industrial (or economic) espionage targeted at the U.S.; the FBI has seen a 53% rise in its cases related to economic espionage within this past year.[4] Many of these cases have been tied to the Chinese government, which has continued to conduct a "planetary scale" cyberespionage campaign against government, military, and commercial targets. China still heavily relies on imported technology, and the country, realizing the need to deepen its modernization, is increasingly doing so through an informal technology transfer apparatus involving many organizations which lie below the export control threshold.[5]

[4] Barrett, Devlin. "U.S. Plans to Use Spy Law to Battle Corporate Espionage." *The Wall Street Journal*, July 23, 2015.

[5] Hannas, William C., Mulvenon, James, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology acquisition and military modernization*. London: Routledge, 2013.

Examples of Chinese Industrial Espionage

Two examples of Chinese industrial espionage against the U.S. bioeconomy have been recently made public. The first example concerns the case of Mo Hailong, a Chinese agriculture company official and U.S. permanent resident, who had been engaged in a scheme of collecting seeds from Monsanto and DuPont test fields in Iowa and sending them back to China, often hiding the material in Orville Redenbacher popcorn tins.[6] The other example concerns two Chinese agricultural scientists, Weiqiang Zhang and Wengui Yan, who stole samples of various seed varieties from a biopharmaceutical company's research facility in Kansas. Both individuals lawfully resided in the U.S. – Zhang, an agricultural seed breeder at the targeted biopharma company, and Yan, a rice geneticist with the U.S. Department of Agriculture. In an attempt to smuggle the seeds back to China, the pair were found out when U.S. Customs and Border Protection located the seeds packed within their luggage.[7] These examples illustrate strong cases of attempted trade secret theft, or bioeconomic espionage, as a means of transferring proprietary material to develop better agricultural products in China.

Data Exfiltration

Beyond just the exfiltration of physical proprietary materials and products from the U.S., data are being exfiltrated at an enormous scale. Notably, the Anthem and OPM data breaches have yet to appear on the dark web, strengthening the assertion that the stolen data are intended for the purpose of espionage rather than commercial gain.

Countermeasures

When faced with data insecurity, Mulvenon offered the following guidance to counteracting espionage: 1) recognize the problem and identify the targeted assets, 2) assign attribution, and 3) go on the offense and actively survey those organizations committing the espionage. Identifying the organization's "crown jewels," or key assets, and critically assessing where that information is stored are important defensive strategies. Specifically, is that information on protected or shared drives? Ultimately, when operating with valuable data, a price will have to be paid in terms of its accessibility and security. Greater investment will need to be made in securing the data, which in turn may require moving it offline, or off of a shared network, and thus rendering it less accessible. These are critical considerations when assessing the value of existing assets.

THE ROLE OF INFORMATICS IN THE BIOECONOMY
Stakeholder Perspectives

SECURITY ISSUES RELEVANT TO HEALTHCARE PROVIDERS

Mr. Seth Feder, Director of Healthcare and Life Science Research at Dell, noted that there are two prime directives in the provider space: 1) capture, store, and guarantee the integrity of healthcare data in perpetuity, and 2) deliver data to validated users with clinically relevant speed and guarantee the authenticity of the data.

Highlighting the first directive, it is acknowledged that the length of time for which you keep healthcare data is not often well defined in the law. In fact, the default is to keep it forever. Oftentimes there is uncertainty surrounding the data's true value, so everything is kept, including for example, raw DNA reads. A single patient's data record can total ~1 terabyte in a given doctor's visit, which gives a sense of the enormity of patient datasets in totality.

[6] Bunge, Jacob. "U.S. Ups Fight Against Agricultural Espionage." *The Wall Street Journal*, April 23, 2015.

[7] U.S. Department of Justice. "Two Agricultural Scientists From China Charged With Stealing Trade Secrets." Press Release, December 12, 2013.

Healthcare providers face two key informatics problems: data rest and data flight. With respect to "data rest," the volume of stored healthcare data requiring classification is immense, and not all data are of equal import, especially with time. The security of stored genomic data is particularly concerning, as it could be a clear target for bad actors. Given the amount of data and extent of time for which data are held, there is a big push for audit logging to monitor who enters/manipulates a data record. Regarding "data flight," the bioeconomy of the future will require moving data outside the firewall, wherein individual provider organizations can obtain information on premises behind the wall.

Feder ended by stating that whatever security solutions are proposed with respect to health-related data, we must remember that we are all ultimately patients and consumers of healthcare. And as patients and consumers, openness, transparency, and fair use of personal data should all be rights to us. With respect to our personal healthcare and genomic data, we should be able to know who is using it and where it is transferred – that is a right we should all have.

BIOSECURITY: EMERGING SYNBIO CAPABILITIES AND NATIONAL SECURITY

Dr. Gigi Kwik Gronvall, a Senior Associate at the UPMC Center for Health Security and an Associate Professor at the University of Pittsburgh School of Medicine and Graduate School of Public Health, provided her remarks from a "user/protector" perspective. Gronvall highlighted four areas of concern in biosecurity affecting the bioeconomy.

1. *Potential misuse of a pathogen for harm (or to manipulate markets)*
   In previous decades, one had to procure a pathogen sample in order to use it. Today, in the era of synthetic biology, direct access to the physical pathogen is no longer required; all that is needed is the genetic sequence and necessary instrumentation with which to synthesize it.

2. *Accidental misuse of a biological organism*
   Accidental misuse of a biological organism yields much of the same effects as deliberate use. Recent examples include the DoD shipment of live anthrax and the discovery of smallpox in an FDA freezer. While both were non-deliberate, these incidents had a significant impact on public perception. Currently, biosafety is underdeveloped in many parts of the world and there are few, if any, existing international norms for its regulation.

3. *Misuse of biological information*
   The (unintentional) misuse of biological information is a real concern. The Biological Weapons Convention (BWC) does not prohibit defensive research, and as such, there is biodefense research performed that is not illegal, but could be potentially damaging, if that work were to be revealed and stolen by bad actors.

4. *Effects of diminished U.S. preeminence in synthetic biology and biotechnology*
   It is important to consider the possible effects of the U.S. falling seriously behind in synthetic biology and other areas of biotechnology. Gronvall stressed that if the U.S. loses its preeminence in these areas, the country risks any future leverage in international treaty and lawmaking in this arena. Further, she noted that many traditional security analysts and foreign policy experts do not consider the bioeconomy to be at the level of national security, a potentially detrimental stance moving forward.

DETECTING SYNTHETIC UNKNOWNS AND GENE GUARDS

Dr. Peter Carr, who leads the synthetic biology research program at the Massachusetts Institute of Technology's Lincoln Laboratory, spoke from a "user-driven" perspective, sharing a couple vignettes highlighting his experience with bioinformatics security issues and strategies to mitigate them.

Carr discussed his work with the DARPA CLIO program centered on gene guards and possible ways to protect IP encoded in the form of DNA. Included among the proposed strategies were DNA disguise, lock and key oriented mechanisms, and xenobiology. Carr also described a small educational project he did for DARPA, where he worked with students to try to identify specific bioengineered DNA signatures in sequences. The goal of this exercise was to determine whether a part of the sequence had in fact been engineered, and if so, what the intended function of that sequence was. The ability to carry out this sort of analysis is important from a defense perspective – ideally, we want to be able to analyze a DNA sequence and identify whether it has been tempered with. If it has, does the engineered sequence have a specific function? And further, what might be the intended use of that function?

A SECURITY FIRM'S PERSPECTIVE

Ms. Melissa Rhoads of Lockheed Martin commented that it is critical for any organization to start identifying its security posture and secure its system(s) from day one. Collectively, we ought to be thinking about security at the population level. Based on the types of data that have been breached (e.g. health records, genomic data), we are now vulnerable to targeted attacks as a population. When organizations think about and collect intelligence in the current security arena, they need to be thinking about actionable intelligence, and particularly, about systems adaptations based on how security might be conducted in the future. Further, academic researchers need greater guidance regarding export control – specifically, the security implications of sharing certain types of data and research among colleagues.

THE ROLE OF INFORMATICS IN THE BIOECONOMY
Roundtable Discussion

DATA SECURITY: EXISTING AND FUTURE PARADIGMS

Encryption vs. Access Control and Management

When considering the efficiency and expected cost-benefit of traditional data security methods, such as encryption, the effectiveness of such methods within the current security context was called into question. Specifically, it was mentioned that at one time, encryption was viewed as a highly effective means of security, but it has proven to still be vulnerable. Additionally, with encryption come the added costs of management and performance, especially for larger organizations. One participant suggested that the focus of securing data should perhaps shift toward access controls and management, until more effective means of encryption, such as homomorphic encryption, become more widely available. Another noted that access controls could also permit more efficient information sharing and collaboration among researchers, particularly with regard to open access data. There was some uncertainty among the group, however, as to whether the security of open access data could ever truly be secure in the absence of complex, layered defenses, which could be counterproductive.

Importance of Organizational Behavior

One participant noted that the companies and organizations which handle security effectively are those where, at the board level, security is explicitly discussed and there is continuous monitoring of security and vulnerability

issues. Specifically, those organizations that are consistently, proactively, and vigilantly looking for and routing out system insecurities are most successful at deterring breaches. The participant noted that these organizations do not deal with attacks as they happen, nor do they use attacks as a means for initiating security reforms. Rather, security is incorporated within the organization's operations and values systems. When asked how many of these types of organizations exist, the participant replied that security is most often discussed and prioritized at the level of the Chief Information Officer, but less than 50% of the time at the board level of a company. Another participant noted that board participation is gaining greater traction within the pharmaceutical sector.

Participants also discussed the role of Information Sharing and Analysis Centers (ISACs), which offer a centralized resource for gathering and sharing information and analysis between the private and public sector on cyber threats to key infrastructure components. ISACs are typically industry-specific, the Financial Services ISAC being one of the most successful and influential. Building off of this concept, one of the participants suggested that communities within the bioeconomy, such as that of synthetic biology, could greatly benefit from an ISAC-like organization or trade group. In such a forum, members could identify potential and existing threats and act as a community to thwart those threats.

Paradigm of Involuntary Radical Transparency

In the wake of several recent significant data breaches and hacks, workshop participants discussed whether communities within the bioeconomy now have reason to ultimately accept that they operate within a context of involuntary radical transparency. In this context, traditional modes of data security and defense lose effectiveness and relevance. Moreover, were a new paradigm of radical transparency to be adopted, the question arose as to whether economic models valuing radical transparency could be constructed? Could radical transparency be reframed in such a way that it was an economic advantage rather than a disadvantage? A participant noted that while the concept has true value, it could be difficult to sell in the current market, as there is significant demand for security services.

Security Measured by Effective Deterrence

Some participants noted that if communities within the bioeconomy resign to the fact that complete security is unattainable, it then becomes a question of the degree to which protection can be provided. Notably, if the costs to non-state actors can be raised to the point where they are deterred, that could be construed as a significant achievement. Operating within this context of inherent insecurity, it is again important to consider the costs and benefits associated with installing added layers of protection, like encryption. In the future, it may be that effective security is redefined from the traditional definition.

Economic vs. Personal Costs: Ascribing Value to Specific Types of Data

During the group's discussion, the value of specific types of data was raised. One participant believed that it was important to distinguish between data that are of economic verses personal value, noting that the costs associated with the loss of certain types of data may not be of comparable value or scale. The OPM hack was raised as an example of what could be construed as a *personal loss* with *personal costs*. It was argued that the OPM hack represented a different kind of security issue than something on the level of a genetic data breach. To illustrate this comparison, one participant noted that unlike certain forms of personal information, such as social security numbers, which are replaceable, genetic data are unique and cannot be replaced.

Acknowledging the uniqueness of genetic data, members of the group proposed ascribing a certain value or cost to an individual's genetic information. Currently, individuals provide their genetic information at no cost (to physicians, researchers, etc.). One participant posited that perhaps genetics should not be free and that potentially a new model allocating value to genetic information could be instituted and made to be the norm. In

this way, perhaps as a society we could change the economics of loss and promote innovative methods of security and government regulation. Building off of these comments, another participant raised the issue of what it would mean to hold aggregate genomic data, and whether companies that hold aggregated data could be held liable.

One participant raised the arguably unique value of pharmaceutical and health data, which were identified as the most expensive data on the black market. The individual noted that for pharmaceutical companies it takes roughly 7-10 years to develop a drug, at a cost of about $1 billion to get it through the testing phases. Because of the time and money investment in drug development, the value of the data generated is that much greater, as are the stakes surrounding its security.

Spectrum of Risk

One participant highlighted the extraordinary depth of the information originating from the bioeconomy and the impressive extent to which that information is shared. There is an extensive amount of data available to those willing to collect it, and it is not entirely known how these data could be used en masse by bad actors. Operating within the existing information revolution and acknowledging that databases can be hacked, yields many uncertainties about the future use of such information. This uncertainty is further compounded by the extraordinary rate of innovation in the biological sphere.

Acknowledging that several of the security issues and risks identified within the bioeconomy are quite nebulous, another participant thought such risks might be better understood if prioritized along a temporal spectrum. Specifically, it was suggested that an effective way of managing and prioritizing threats could be to align those threats along a timeline of expected incidence. In this way, mitigation tactics could be strategically considered and deployed at the appropriate times.

A participant noted that, in the future, one mitigation technique could in fact be to continually accelerate the rate of innovation in the bioeconomy – to innovate at a rate that is unmatched and insurmountable by bad actors and global competitors. The participant noted that the U.S. bioeconomy is facing an arms race in terms of who has the largest and most diverse datasets. Moving forward, the participant said, it will be important to address the security aspects of informatics, while simultaneously facilitating innovation and maintaining the global competitiveness of the U.S.

Maintaining Global Leadership and Competitiveness

During the discussion, participants mentioned the role of the U.S. as a global leader in championing bioeconomy security issues, and questioned whether the nation has the responsibility to bring awareness and visibility to these issues. One participant noted that these discussions had not been previously raised during S&T discussions in international collaborations, but should be made a priority and brought to the table. Another participant noted that, ultimately, any policies developed within the U.S. with the intention of bolstering data and information security within the bioeconomy will need to have meaningful impact and translate globally. The participant went on to say that it is clear that increasing awareness that this is even an issue, both domestically and internationally, is one of the many things that need to be addressed.

CRIMINAL THREATS AND VULNERABILITIES IN THE EXISTING AND NEAR-FUTURE BIOECONOMY
Mitigating Risk, Promoting Adaptation and Innovation

Six discussants individually presented their thoughts on the types of criminal behavior that exist within the bioeconomy, how such criminal behavior is enabled, how it might be contained, and how to adapt responses when formerly criminal activities become legal. Discussants' commentary identified existing challenges with safeguarding research and innovation in academic and industrial settings; in particular, balancing the need to mitigate criminal activity, while not constraining advancement.

OPPORTUNITIES AND THREATS IN NEUROBIOLOGY AND SYNTHETIC BIOLOGY

Dr. Andrew Ellington, Professor of Chemistry at the University of Texas at Austin and planning committee member, provided an introductory talk to the session. Ellington's presentation highlighted the tremendous advances in the fields of neurobiology, synthetic and systems biology, while simultaneously identifying the unanticipated consequences, threats, and vulnerabilities of advancing technologies and knowledge in these areas.

Neurobiology and Synthetic Biology Explosion

There has been an explosion of knowledge and discoveries in the field of neurobiology much enabled by advances in systems biology. Through the application of systems biology principles, we have been able to generate genetic and other types of data for an amazing number of organisms. By integrating these data, we can generate a probabilistic view of function within and between organisms. Such holistic systems knowledge enables us to perform drug screens and fosters drug discovery. Further, the tremendous advancements made in synthetic biology have greatly expanded the engineering capability of many materials, providing even small university laboratories with extraordinary synthesis capabilities.

Unanticipated Consequences

Ellington cautioned that with this impressive advancement and innovation come unanticipated consequences. We are now operating in an ethically, scientifically, and legally grey area. The deliberate and non-deliberate adulteration of biologicals and chemicals is especially concerning looking to the future. As an example, vaccines could unintentionally drive disease; specifically, with immunization, strains could evolve to become more virulent and possibly overcome the protection offered by a vaccine.[8] Improved genetic testing could offer a potential means of both avoiding unanticipated consequences and liability.

SAFEGUARDING UNIVERSITY RESEARCH ON THE BIOECONOMY

Dr. Graham Carr, Vice-President for Research and Graduate Studies at Concordia University in Montreal, Quebec, Canada presented his remarks on a recent, collaborative study between Concordia University and the University of California, Berkeley, in which yeast was engineered to convert sugar to opiates, such as codeine and morphine.[9] Concurrent with the study's findings being published in *Nature Chemical Biology*, the journal *Nature* published a commentary piece arguing that the existing regulatory environment was ill-equipped to deal with such breakthrough science. Subsequent publicity surrounding the article was largely focused on the

[8] DeLoache, William C. et al. "An enzyme-coupled biosensor enables (*S*)-reticuline production in yeast from glucose." *Nature Chemical Biology* 11 (2015): 465-471. doi:10.1038/nchembio.1816.

[9] Concordia University. "Beyond the poppy: a new method of opium production." Press Release. May 18, 2015.

criminal scenarios of home brewed heroin and the existing national and international regulatory deficiencies. Ultimately, the coverage paid little attention to the potential positive impacts this innovation could have on the economy and human health; the social innovation piece of the story was buried.

Carr's story highlighted the existing challenges associated with safeguarding university research on the bioeconomy, particularly involving disruptive technologies. The opiates discovery has sparked important questions concerning the physical security of university laboratories – in terms of their accessibility, equipment and technology, and materials. At Concordia, not unlike many universities, the synthetic biology laboratory has, until now, had a low level of security having purposely been designed to be an "open bench," building on the principle that open access is fundamental to nurturing learning, inquisitiveness, and innovation. The recent scientific breakthroughs, together with possible lay (mis)perceptions of lab activities arising in light of media coverage, have highlighted questions about screening and security to prevent misuse of equipment or materials for illicit purposes.

Carr also emphasized that while the opportunity to commercialize research necessitates the protection of information, universities increasingly operate within an open access data environment, where the results, data, and metadata of publicly funded research are expected to be made public. However, because research data management and information security are seldom comprehensively addressed across all domains of university research, major points of vulnerability exist on most campuses. Safeguarding university research on the bioeconomy in the context of disruptive technologies is a topic that requires greater prominence and vigilance.

TOOLS TO SAFEGUARD AGAINST INDUSTRIAL ESPIONAGE

Dr. Patrick Boyle, Design Group Leader at Ginkgo Bioworks, presented tools designed to prevent industrial espionage from the perspective of a synthetic biology company. Within companies such as Ginkgo there are two primary assets: the foundry and the genetic codebase. The foundry, the physical factory where engineered organisms are designed, built, and tested, is inherently complex and hard to replicate, and has known protections. In contrast, the genetic codebase, which is proprietary information of the company, is much harder to protect once it is incorporated within the engineered organisms deployed by the company. Two of the mechanisms currently used to protect such organisms from industrial espionage include lock and key mechanisms and gene guard systems. While simple systems of protection do exist, moving forward, better systems will need to be developed and integrated.

SAFEGUARDING SYNTHESIS: AN ONTOLOGICAL APPROACH

Dr. James Diggans, Director of Biosecurity for Twist Bioscience, remarked on the means and significance of safeguarding (DNA) synthesis. Synthesis efficiency (and, as a result, design iteration) is limited by existing sequence screening processes and human interpretation of results. Further, scaling biosecurity screening is currently quite challenging. For large-scale synthesizers, biosecurity screening technology is computationally expensive and has a high (~5%) false positive rate. And, for smaller companies, there is no open resource for biosecurity screening. Overall, there is no comprehensive mapping of sequence to risk, which is a pressing need. The existing Select Agent and other regulatory frameworks define risk at the level of a whole organism or broad categories of pathogenicity, but not at the sequence level.

Diggans remarked that we need an ontology of sequence-based risk that considers whether the sequence bears risk to the community or the individual; who or what is at risk; whether are there specific conditions or routes of sequence transmission; whether the sequence is necessary or sufficient for pathogenicity; and whether there could be synergistic effects with other biological systems. With this information, regulatory frameworks could be

defined in ontological terms and thus leave far less ambiguity. Plausible steps for safeguarding synthesis include 1) developing an ontology defining biological risk; 2) leveraging distributed expertise to annotate known sequences using the ontology with roles in pathogenicity; and 3) funding development of advanced screening techniques using this new metadata.

BIOLOGICAL COUNTERFEITING IN PHARMACEUTICALS

Thomas Kubic, President and CEO of the Pharmaceutical Security Institute, offered remarks on the increasing incidence of biological counterfeiting within the existing, legitimate global marketplace. Specific biologics have frequently been targeted for counterfeiting including those used in cancer and hormone therapies. Common forms of counterfeiting include reuse of the original bottling with a substitute product, alteration of expiration dates, and up-labeled dosages on medication labels. In 2013, most counterfeits originated in China, Columbia, Brazil, Mexico, and Russia. Notably, with the rise of the Internet, there has been an increase in the shipment of these products globally. Kubic commented that while there is a good surveillance system in the U.S., the risk of procuring counterfeit medications through the Internet still remains high, translating to increased security and health risk for the population.

ILLEGAL NETWORKS AS SELF-LIMITING ENTITIES

Henry Farrell, Associate Professor of Political Science and International Affairs at the George Washington University, offered commentary on illegal networks operating on the dark web. Notably, Farrell presented a counterargument to popular assertions that these illegal networks pose significant threat, arguing that many of these networks will be self-limiting due to inherent issues of distrust that exist within them. Additionally, as law enforcement in this arena becomes more successful, a heightened sense of paranoia within the networks only generates further suspicion. Because of this, actors within illegal networks are more interested in short-term versus long-term activities.

Challenging the self-limiting nature of illegal networks, one participant disagreed that distrust alone within these groups would be sufficient to constrain or deter their capabilities. The participant continued by stating that these bad actors would not leave the marketplace due to mistrust, rather they would continue their illicit behavior by seeking out other, more reliable partners.

SECURITY ADAPTATIONS FOR EMERGING INDUSTRIES

Meg Sanders, Chief Executive Officer of MiNDFUL, a Colorado-based cannabis producer with medical and recreational dispensaries, spoke to the security adaptation requirements and responses required in the face of newly legalized controlled substances, such as cannabis. Currently, there is limited to nonexistent legal and regulatory protections for research and development within the cannabis industry, including the inability to patent the technology and methods. There is concern that in the absence of such protections, the security of the plants and production materials could be greatly compromised. Further, it is possible that the U.S. may miss out on important opportunities to expand health-related therapies rooted in cannabis treatments, and thus may fall behind other countries in advancing this technology.

CRIMINAL THREATS AND VULNERABILITIES IN THE EXISTING AND NEAR-FUTURE BIOECONOMY
Roundtable Discussion

Building Networks of Trust

Building off of Henry Farrell's discussion of the self-limiting nature of illegal networks, one participant proposed that a potential means to safeguarding the bioeconomy might be for its stakeholders to build firm networks of trust, while continuing to operate in the context of radical transparency. In theory, if the various subgroups of the bioeconomy can build out their trusted networks with which they collaborate and do business, the impact of bad actors could be much reduced. Another participant noted the importance of reputation in achieving these trusted networks, especially within the marketplace. In the absence of a regulatory body, these networks and markets must rely on the reputations of those with whom they do business. In this way, reputation, in the absence of government regulation, could offer a natural means of self-regulation. Another participant noted that a means of showing or proving that a given entity has a quality product is needed to create trusted buyers and sellers, and instill confidence within the market.

During the discussion, self-identification of risk was raised as an important means to containing existing or preventing future threats to security in the bioeconomy. In particular, creating a culture of communication and information sharing within the communities of the bioeconomy would be an important step to mitigating risk. One participant pointed out that the researchers and administration at Concordia University and UC Berkeley were praiseworthy in their early efforts to identify the potential risks and implications of their published research, as well as in their attempts to mitigate that risk. The participant went on to say that communities within the bioeconomy ought to emulate this sort of action more broadly by self-identifying areas of high risk or vulnerability.

Safeguarding Synthesis

One participant posited if barcoding DNA sequences might be a plausible means of tracking those sequences within deployed engineered organisms. In theory, with such technology, any illicit transactions involving the barcoded sequence could be identified and traced. Another participant responded by stating that the challenge with barcoding DNA is that the process often breaks the functionality of the sequence itself. Further, the barcoding process is very difficult to achieve without deep knowledge of sequence design.

Another participant brought up the point that screening for "bad" or threatening DNA sequences is not necessarily related to biosecurity per se. Rather, a big driver of sequence screening is for protection from corporate liability. This participant said that to call screening a "security concern" alone was a misnomer, but rather, it should be thought of as a conscious raiser.

Current Investment in the U.S. Bioeconomy

During the discussion, one participant raised the importance of dedicated investment as a necessary means to safeguarding the U.S. bioeconomy. Specifically, the participant commented on the remarkable investment China has made in its students and training within the bioeconomy. This is particularly true in the area of data analytics. While graduate students in the U.S. do receive some data analytics training, it is rather limited in scope. Only a small fraction of U.S. biology Ph.D. students have a rigorous quantitative analysis component to their program, compared to biology Ph.D. students in China. The participant went on to express doubt about the extent to which the U.S. is investing in the future of its bioeconomy. The participant stated that, to safeguard the future bioeconomy, requires looking at where our investments in the bioeconomy become a realization. In this way, lack of investment in our graduate students could translate to a missed opportunity for the U.S.

SECURING AND FLOURISHING THE BIOECONOMY FOR THE FUTURE
Existing Challenges and Future Priorities

WHAT MIGHT KEEP THE BIOECONOMY FROM DELIVERING ON ITS PROMISE?

Dr. Roger Brent, a Member of the Division of Basic Sciences at the Fred Hutchinson Cancer Research Center and workshop planning committee member, highlighted the existing IT landscape and security environment within the bioeconomy. Brent identified what he sees as the current systemic threats and vulnerabilities within the IT sphere, and commented on the accepted, but potentially insufficient, framework used to deter data thefts and other cyberattacks.

Characteristics of the Current IT Security Environment

The informatics component of the current bioeconomy is vast, including a wide array of digital information that is often stored indefinitely. Due to the complex and constantly changing nature of the software, network, and human systems managing these enormous swaths of data, these systems are bound to contain vulnerabilities that are effectively unknowable. An attacker can ultimately choose the target and time of the attack. Moreover, many attacks bear little cost to the perpetrator; this is largely due to the fact that there exists limited ability to identify the perpetrators themselves. In the current IT security environment, with sufficient time and resources, any perimeter and system can be breached.

Strategy for Deterring Cyberattacks Requires a Dedicated Policy Framework

For these reasons, one key means to prevent cyberattacks depends on deterring them. The classical components of a deterrence strategy include reducing the likelihood of the attacker's success and increasing the perceived cost to the attacker. Successful deterrence requires detection of attacks, response to them, and mechanisms to recover from them. The response portion of a deterrence strategy requires policy and technology that enables retaliatory responses that are meaningful, proportionate, targeted, and accurate. The technology is too complex to improvise, and thus needs to be pre-assembled and ready to be deployed when needed.

Brent commented that the DoD has announced a doctrine for responses to cyberattacks and that, according to its criteria, most or all of the recent attacks on the bioeconomy would not warrant a response from DoD. It seems that the U.S. currently lacks a policy framework for the kinds of affirmative responses that might have deterred recent attacks and reasonably anticipated future attacks on the bioeconomy.

CAUSES AND COUNTERMEASURES TO DATA INSECURITY

Dr. Richard Danzig, a Director of the Center for a New American Security, offered a commentary on what he views are the technical difficulties that have given rise to the current vulnerabilities seen within the IT sphere of the bioeconomy.

Root Causes of Digital Insecurity

Danzig attributes the root cause of digital insecurity predominantly to three, interconnected concepts: information concentration, connectivity/communicability, and complexity. It is the pooling of information that is so fundamental to the power of cyber or digital systems. For a given amalgamation of information, the greater the extent of connectivity and complexity within these systems, the more opportunities there are for the systems' penetration and exploitation. Importantly, the cause of digital insecurity goes beyond the risks associated with software; external (and sometimes inadvertent) risks pose a threat, including supply chain

issues, insiders (e.g. Edward Snowden, third party contractors), social engineering, and mismanagement (i.e. configuration and password sharing issues).

Building Defensive Capabilities and Countermeasures
Danzig stated that one of the critical issues with the U.S. government's current posture towards thwarting cyberespionage is that it is "offensive heavy." The current investment in offensive capability and defenses would be benefitted by greater investment in defensive capability and strategy. While the existing offensive countermeasures provide degrees of protection against lesser attackers, in the long run, they leave systems vulnerable to high-end attackers. The key is to understand and accept the broad vulnerability that exists within our cyber systems and to build resilience (i.e. defensive mechanisms) into the systems to more effectively recover from and deter, if not thwart, future attacks.

GOVERNANCE OPPORTUNITIES IN THE BIOECONOMY

Mr. Benjamin Wittes, Senior Fellow in Governance Studies at The Brookings Institution, led a discussion of governance opportunities in the U.S. bioeconomy, addressing the plausibility of creating governance and regulatory frameworks that would ensure a secure environment in which the bioeconomy could flourish. Overall, ultra-complex regulatory environments, such as the bioeconomy, are not utterly hopeless in the government sphere. Rather, if approached incrementally, regulations can be very powerful and lead to a better, albeit more challenging, environment.

Wittes offered a few examples to demonstrate success in regulating highly complex and sometimes high risk environments, including China's effective regulation of the Internet in its country, regulating driving in America, and building codes. Applying these ideas to the bioeconomy, Wittes clarified that the same set of regulatory structures and practices should not be created to protect the various threats that exist within the bioeconomy (e.g. genomic identity threats, IP threats, etc.). Rather, each major area of threat ought to be thought of as a different entity, and thus, a different regulatory issue. In developing regulatory mechanisms for each threat, Wittes suggested the following: 1) disaggregate the problem; 2) consider all the possible actors and all levels at which behavior can be regulated; and 3) identify how liability risk will be allocated. Wittes highlighted this last point as critical to the process; notably, every functional, complex regulatory system has determined how and to what parties liability risk will be assigned. In the bioeconomy, it will be critical to determine how risk is defined and assessed within such a diverse space, and moreover, how risk and liability will be allocated in the face of novel applications.

SECURING AND FLOURISHING THE BIOECONOMY FOR THE FUTURE
Roundtable Discussion

Global Norms of Governance/International Considerations
In light of the discussion surrounding governance and regulation of the bioeconomy, one participant commented on the importance of building regulatory mechanisms that function in a global context. The participant cautioned that achieving consensus on biotech issues within the United Nations can already be an excruciating process and is often very difficult to achieve. In working towards norms of governance or regulation for the bioeconomy, global applicability of those principles is an important consideration. Further, governance mechanisms that will not only safeguard the bioeconomy, but also enable it to flourish and grow nationally and internationally are similarly imperative, added the participant.

During the discussion, some participants also reflected on the importance of monitoring the jargon used when speaking about the bioeconomy in international settings. It was noted that different countries have different ethics and sensitivities towards the various sub-disciplines of the bioeconomy, such as synthetic biology. Moreover, the bioeconomy itself has been defined quite differently around the world, with the U.S. and China maintaining the broadest definitions.

Significance of Small/Medium Enterprises

In considering potentially notable influencers of law or licensure within the bioeconomy, one participant urged that the group be sensitive to the incredible power dynamics of economies of scale. Specifically, the participant noted that a large part of the bioeconomy is driven by start-ups and small and medium enterprises, and that their ability to influence any putative laws or licensing would be of a different scale (than that of the traditional, large corporate firm). As such, it would make sense to exercise some sensitivity when involving these key stakeholders in any decision-making process.

Non-traditional Regulatory Mechanisms

One participant raised the concern that government issued regulations tend to be formulated and amended at a rather slow pace, and as such, could be counterproductive to a rapidly growing bioeconomy. Instead, the participant suggested, other non-traditional regulatory mechanisms could be considered as an effective means of governing the safe creation of an environment in which the bioeconomy could flourish. The participant cited public image and perception as potentially strong regulators of behavior and ultimately suggested looking for ways in which the system, in its existing state, could be made to work [regulate] to one's advantage.

Safeguarding the Bioeconomy: A Spectrum of Risk

Given the vastness and distributed nature of the existing, and continually growing, bioeconomy, one participant observed that it might be necessary to consider at what level and which specific aspects of the bioeconomy could be reasonably safeguarded. Building off of this, another participant returned to the idea that different types of data lie along a spectrum of risk, and as such, can be ascribed different valuations depending on where they lie along that spectrum. That same participant highlighted that within the current global bioeconomy, "the largest, most diverse dataset wins." In this context, individual genomes would not be considered "high risk" or of "high value." However, as part of a whole (i.e. a larger dataset on the population level) individual genomes are much more powerful and influential, and thus bear a greater security risk.

In response to these ideas, another participant noted that the value of any individual genome is not clearly black and white; rather, it is difficult to say at any point in time that an individual's genome may or may not be important. This participant emphasized that there is an important temporal component to be considered. For example, were someone to become the President of the United States or the CEO of a major corporation, their genomic information now has significant value, when it may not have previously.

Another participant reiterated that the citizen's loss of personal empowerment is an inherent vulnerability of the bioeconomy, which could be remedied by monetizing health and genomic data. The participant went on to state that when individuals have greater personal empowerment, they are able to bargain more effectively both individually and collectively on their own behalf – potentially leaving the system less vulnerable to collapse and failure.

APPENDIX A
WORKSHOP AGENDA

Workshop on Safeguarding the Bioeconomy: Applications and Implications of Emerging Science

July 27–28, 2015

National Academy of Sciences Building
2101 Constitution Avenue NW, Washington, DC
NAS Lecture Room

A bioeconomy is one based on the use of research and innovation in the biological sciences to create economic activity and public benefit.

-National Bioeconomy Blueprint, White House, April 2012

MONDAY, July 27, 2015

8:30 – 9:00 a.m. **Welcome, Introduction, and Purpose of the Workshop**
Richard Johnson, Chair of Workshop Planning Committee
Edward You, FBI

9:00 – 9:15 a.m. **Overview of the Bioeconomy**
Douglas Friedman, The National Academies of Sciences, Engineering, and Medicine

9:15 – 9:45 a.m. **Keynote Address: "Industrial Espionage: The Theory and Practice of Breaches"**
James Mulvenon, Defense Group Inc.

SESSION 1: ROLE OF INFORMATICS IN THE BIOECONOMY
Richard Johnson, Moderator

9:45 – 10:45 a.m. **Initial Remarks**
For the first part of the morning, a diverse selection of leaders will provide remarks and identify key bioeconomy data/bioinformatics security issues from both a "user-driven" perspective and from a "provider and/or protector" perspective.

Discussants:

- **Traditional Security Firm's Perspective**
  Melissa Rhoads, Lockheed Martin
- **Security issues relevant to healthcare**
  Seth Feder, Dell Inc.
- **Detecting synthetic unknowns and gene guards**
  Peter Carr, MIT
- **Biosecurity: emerging synbio capabilities and national security**
  Gigi Kwik Gronvall, UPMC Center for Biosecurity

10:45 – 11:00 a.m. **Break**

11:00 – 12:30 p.m. **Roundtable Discussion with Workshop Participants**
The second half of the morning will include roundtable discussions with workshop participants.

12:30 – 1:30 p.m. **Working Lunch**

SESSION 2: CRIMINAL THREATS AND VULNERABILITIES IN THE EXISTING AND NEAR-FUTURE BIOECONOMY
Andrew Ellington, Moderator

1:30 – 1:40 p.m. **Introduction on Session 2**
Richard Johnson, Chair of Workshop Planning Committee

1:40 – 2:00 p.m. **Opportunities and Threats in Neuromodulatory Compounds**
Andrew Ellington, Planning Committee Member

2:00 – 3:00 pm **Initial Remarks**
For the first part of the afternoon, key leaders will provide remarks and identify the most important vulnerabilities and nontraditional threats and attacks.

Discussants:

- **Brewing bad: Making known drugs more easily.**
  Graham Carr, Concordia University
- **Synthetic capabilities**
  James Diggans, Twist Bioscience
- **Biological counterfeiting in pharmaceuticals.**
  Thomas Kubic, Pharmaceutical Security Institute
- **Legal networks, marijuana**
  Meg Sanders, MiNDFUL
- **Illegal networks**
  Henry Farrell, George Washington University

- **Tools to prevent industrial espionage from company perspective**
  Patrick Boyle, Ginkgo Bioworks

3:00 – 3:15 p.m. **Break**

3:15 – 4:45 p.m. **Roundtable Discussion with Workshop Participants**
The second half of the afternoon will include roundtable discussions with workshop participants.

4:45 p.m. **Instructions and Questions for Participants to Consider for Session 3**

5:00 p.m. **Adjourn for the day**

TUESDAY, July 28, 2015

SESSION 3: SECURING AND FLOURISHING THE BIOECONOMY FOR THE FUTURE
Roger Brent, Moderator

8:30 – 8:45 a.m. **Review of Previous Day's Discussions**
Richard Johnson and/or Andrew Ellington, Planning Committee Chair/Member

8:45 – 8:55 a.m. **Framing the Third Session: What Might Keep the Bioeconomy From Delivering on Its Seeming Promise?**
Roger Brent, Planning Committee Member

8:55 – 9:15 a.m. **Keynote Address: The Great Data Robbery**
Richard Danzig, Center for a New American Security

9:15 – 10:45 a.m. **Roundtable Discussion: Consequences and Ramifications of the Current Post-Robbery State of Affairs**
Roger Brent, Moderator
Benjamin Wittes, Brookings Institution, Co-Moderator

Discussants from Day 1 will engage in a guided, wide-ranging discussion with federal stakeholders and other invited guests.

Question to consider:

- Assume that the informatic side of the bioeconomy is or will soon be in a state of involuntary radical transparency for all motivated nation-states and possibly other actors: What are the consequences of this to the function of the bioeconomy if its IT components do not become opaque again?

10:45 – 11:00 a.m. **Break**

11:00 – 12:45 p.m. **Roundtable Discussion (continued): Are there Positive or Ameliorative Steps We Might Take – Right Now and/or Long Term?**

Questions to consider:

- Are there any technical fixes for the issues mentioned earlier? Are there any policy fixes? Are there any constructive actions the government, policymakers, or other stakeholders can take?
- Are there any lessons to be learned from the criminal and fringe parts of the bioeconomy about how to maintain an ability to generate new ideas in the presence of some level of ongoing data robbery?
- Any thoughts or speculations for the FBI or other parts of the US National Security community as to how they should view things? What actions they should take?

12:45 p.m. **Closing remarks**
Richard Johnson, Roger Brent, and Andrew Ellington, Workshop Planning Committee

1:00 p.m. **Adjourn**
Thank you for participating in the workshop.

APPENDIX B
WORKSHOP PARTICIPANTS

Matthew Bender, U.S. Government
Patrick Boyle, Ginkgo Bioworks
Roger Brent, Fred Hutchinson Cancer Research Center*
Graham Carr, Concordia University
Peter Carr, Massachusetts Institute of Technology
Susan Coller-Monarez, Office of Science and Technology Policy
Genya Dana, U.S. Department of State
Richard Danzig, Center for a New American Security
James Diggans, Twist Bioscience
Andrew Ellington, University of Texas at Austin*
Gerald Epstein, U.S. Department of Homeland Security
Henry Farrell, The George Washington University
Seth Feder, Dell Inc.
Elizabeth Finkelman, National Academies of Sciences, Engineering, and Medicine
Douglas Friedman, National Academies of Sciences, Engineering, and Medicine
Nalneesh Gaur, PricewaterhouseCoopers
Gigi Kwik Gronvall, UPMC Center for Biosecurity
John Hannan, Defense Threat Reduction Agency
Richard Johnson, Global Helix LLC*
Thomas Kubic, Pharmaceutical Security Institute
Patrick Lincoln, SRI International
Eric Moore, Defense Threat Reduction Agency
James Mulvenon, Defense Group Inc.
Melissa Rhoads, Lockheed Martin
Meg Sanders, MiNDFUL
David Shepherd, U.S. Department of Homeland Security
Katherine Sixt, Institute for Defense Analyses
Steve Williams, U.S. Environmental Protection Agency
Benjamin Wittes, Brookings Institution
Dave W., U.S. Government
Peggy Tsai Yih, National Academies of Sciences, Engineering, and Medicine
Edward You, Federal Bureau of Investigation

* *Member of the workshop planning committee*