Wilson Briefs | March 2016

# How Our Unhealthy Cybersecurity Infrastructure Is Hurting Biotechnology

Wilson Center

by Eleonore Pauwels and Apratim Vidyarthi


## SUMMARY

Recent security breaches in the data of health care providers and governments point toward a larger problem for the biotechnology sector, which on average has been growing more than 10 percent per year over the past decade—much faster than the rest of the economy. Current cybersecurity policy, however, neglects the biotech industry, endangering not only the growth of business but also the infrastructure underpinning the future of life sciences.


As Silicon Valley expands and digitizes everything from our hospital records to our DNA, much more is at stake than even our Social Security numbers and credit card information. The cybertheft of our most sensitive genetic data could be exploited for insurance fraud or identity theft, or lead to a disturbing invasion of patient privacy. But the collective threat posed by cyberattack on our biotechnological infrastructures is even more important.

## Protecting Digital DNA: A Collective Responsibility

Through two executive orders signed February 9, 2016, President Obama implemented a plan to fortify the government's defenses against cyberattacks and protect the personal information that the government keeps about its citizens. The Cybersecurity National Action Plan is supported by a proposed 2017 budget that includes $19 billion for information technology upgrades and other cyber initiatives.[1] The president's strategy, a massive step toward remedying today's lack of a legally mandated coordinated computer security policy, could be viewed as comprehensive if our data were simply physical objects or computer files. But as biotechnology becomes digital, scientists have learned to treat living cells like complex packages of digital information where DNA acts as a computing language. The genetic code that that transfers an organism's genetic characteristics can be stored in a computer, transmitted, and modified just like any other digital information. With the right machines, DNA can be chemically recreated and inserted into what amounts to a blank cell, and booted up—growing cells that have the specified DNA. In March 2016, the renowned biologist Craig Venter announced that his team, which had created the first synthetic bacterial cell in 2010, had become the first to build a synthetic cell with the smallest known genome of any living organism.[2]

Our DNA is a special kind of data, and we do not yet comprehend the implications of losing control of what it reveals about ourselves. On a personal level, for example, it could reveal susceptibility to certain diseases. But on wider levels, the risks of an incomplete cybersecurity policy could endanger an entire industry. If biotech companies were to lose sensitive genetic data, see a medical device hacked, or see their medical data held hostage (as happened recently to a Los Angeles hospital), the outcry could break the industry, costing thousands of hard-gotten jobs in the process and giving China, India, and Europe a competitive advantage.[3]

The president's cybersecurity policy generally protects companies with sensitive data, especially those in Silicon Valley—the very same companies that rise and fall like the tide. But the multibillion-dollar biotechnology industry, which has taken more than 30 years to grow and begin to create genuine scientific advancement, is fragile. A cybersecurity policy that does not engage such an important industry endangers not only the growth of business, but also the creation of a secure infrastructure for the future of life science.

---

1 See "FACT SHEET: Cybersecurity National Action Plan," White House Office of the Press Secretary, February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

2 Rachel Feltman, "This Man-Made Cell Has the Smallest Genome Ever — but a Third of Its Genes Are a Mystery," *Washington Post*, March 25, 2016, https://www.washingtonpost.com/news/speaking-of-science/wp/2016/03/24/the-creators-of-the-first-synthetic-life-made-a-cell-with-just-enough-genes-to-survive/.

3 Larry Greenemeier, "Cyber Thieves Hold Hospital's Data for Ransom," *Scientific American*, February 23, 2016, http://www.scientificamerican.com/podcast/episode/cyber-thieves-hold-hospital-s-data-for-ransom/.

## Biotechnology and the Rise of Cyberespionage

Cyberespionage has already had impact, as in the recent hackings of health insurer Anthem and of the Office of Personnel Management. Further dangers are notable. For example, a company like Ginkgo Bioworks, which recently won a "small" investment of $45 million, makes money out of creating "custom-made organisms" from digital genetic codes it has built. Protecting these codes from industrial espionage, once they are incorporated in engineered organisms, is extremely challenging because as the engineered organism is shipped out to clients, its genetic instruction code can be copied, costing millions in lost revenue.

For another example, San Francisco–based Emerald Therapeutics offers virtually any scientist access to a lab in the cloud where automated robots conduct experiments exactly as specified by the user. In a nutshell, from a laptop (in a coffee shop), a scientist can log in to Emerald Therapeutics software and design an experiment—for example, designing an oncolytic virus for use in cancer therapies—and the company will ship the samples as well as save the data experiment in the cloud.[4] This revolution in how we think about and manage biotechnology is vulnerable to data theft, unethical modification of experiments, and building of biological organisms that genuinely could be considered a weapons of mass destruction threat.[5]

## Recommendations

Anything that touches biotechnology relies on computing—commercial gene banks, fingerprint data, health data, facial recognition data, and medical machines. Such technologies are poised to become intrinsic to our lives in the future. If, in the future, our DNA—the very program that regulates the functioning of our cells—and everything related to it is located somewhere on a computer, securing that data must be the first priority as we incorporate biotech into our everyday lives. Now that President Obama has released his cybersecurity agenda, the time is ripe to extend it to the growing needs of a digital biotech industry.

- As the number of annual data breaches begins to accelerate, biotech companies need to be incentivized to develop cybersecurity architecture.[6] One way would

4 See the explanation of the Emerald Cloud Lab on the Emerald Therapeutics website at http://emeraldcloudlab.com/how-it-works.

5 Antonio Regalado, "Top U.S. Intelligence Official Calls Gene Editing a WMD Threat," *MIT Technology Review*, February 9, 2016, https://www.technologyreview.com/s/600774/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/.

6 "2016 Trend Micro Security Predictions: The Fine Line," *Trend Micro*, October 27, 2015, http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016.

be to follow the example of the latest data laws in California, which require that government data breaches be reported to customers.[7]

- Biotech companies should develop specific standards of encryption for activities related to genome sequencing and storage, akin to higher levels of security for personal data. Such standards need to be required throughout the industry, and need to be continuously updated.
- The U.S. government should consider creating a cyber–Centers for Disease Control and Prevention that could create forums for biotechnology companies specifically dedicated to sharing information about threats and designing collectively a cybersecurity architecture that would prevent future disasters. Such architecture must anticipate the growing need for cloud computing beyond the capabilities of current internet systems.
- The U.S. government could mandate gene guard systems, which protect the information encoded in DNA by helping to detect any tampering with genetic sequences.
- Finally, as the demand and research on genomic sequencing, gene banks, and DNA editing increases, consumers must be educated on the caveats and risks involved in these services.

---

7 Kim Zetter, "California Now Has the Nation's Best Digital Privacy Law," *Wired*, October 8, 2015, http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

Eleonore Pauwels is senior program associate with the Science and Technology Innovation Program at the Wilson Center.

Apratim Vidyarthi is a researcher in the Engineering and Technology Innovation Management Program at Carnegie Mellon University.

**The Wilson Center**

@TheWilsonCenter
facebook.com/WoodrowWilsonCenter
www.wilsoncenter.org

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027