Hacking DNA Sequences: Biosecurity Meets Cybersecurity

By Alex Berezow, PhD — January 14, 2021

Vulnerabilities in cyberbiosecurity are becoming a major public health threat. It's time to prepare before the worst happens.

Until recently, biosecurity and cybersecurity have been considered separate realms. The former dealt mostly with preventing dangerous pathogens from escaping labs or falling into the wrong hands, while the latter dealt mostly with preventing hackers from accessing data or stealing money.

But that is now changing. Recent events have shown that there is substantial overlap between these two security concerns. For lack of a better term, those in the field are now calling it cyberbiosecurity.

Consider what has occurred during the COVID-19 pandemic. Hackers used ransomware -- malicious software that holds an organization’s computer files hostage until the hackers are paid a ransom -- to target hospitals [2]. Other hackers stole data [3] about the Pfizer/BioNTech vaccine, which was then released online [4] a month later. Still, other hackers sponsored by Russia, China, Iran, and North Korea [5] were looking to steal COVID vaccine intellectual property.

Given the pervasiveness of such threats, it won't be long before a cyberattack intentionally kills somebody. In fact, one cyberattack in Germany already indirectly killed a patient seeking emergency services but was turned away by the hospital due to a computer network failure. Unable to get treatment in time, she died. It is clear, therefore, that cyberattacks are a threat to public health.
Cyberbiosecurity: Hacking DNA Sequences

A letter to the editor [7] by Dr. Rami Puzis et al. in Nature Biotechnology explains how malware could be used to pull off an elaborate trick: DNA sequence hacking. Ordering short pieces of DNA is extremely common. (I’ve done it myself many, many times when I was a graduate student.) A company synthesizes the DNA, places it in a small vial, and ships it to the lab using a courier like DHL. Once it arrives, the researcher simply adds water, and the DNA is ready to go.

The authors worry that an order for a DNA sequence could be hacked. Specifically, their concern is that -- unbeknownst to the researcher -- a harmless DNA sequence could be replaced with something malicious, say, the DNA sequence for a toxic protein or a virus. Then, when the researcher uses the DNA inside of a cell, out pops a nasty surprise rather than whatever the researcher had hoped to produce. The following diagram depicts how something like this could happen.

This trick sounds way too difficult to be a realistic threat, like it should be the villainous plot of
some *Mission Impossible* movie. But the authors gave it a try and *actually pulled it off* using malicious DNA that encoded a toxic protein. The researchers then canceled the order before the manufacturer synthesized the DNA.

**The Future of Cyberbiosecurity**

There are many areas of overlap between traditional cybersecurity and biosecurity. Another paper [8] written by Dr. Laura Richardson *et al.* in *Frontiers in Bioengineering and Biotechnology* enumerated them.

We have been warned. It's time to prepare before the worst happens.