The next pandemic could be downloaded from the internet

February 4 2014, by Andrew Snyder-Beattie

Too much information could be a recipe for disaster. Credit: Abode of Chaos

Last October, scientists in California sequenced the DNA for the "type H" botulinum toxin. One gram of this toxin would be sufficient to kill half a billion people, making it the deadliest substance yet discovered – with no antidote. The DNA sequence was not placed on public databases, marking the first time genetic code has been withheld from the public over security concerns.

As biological discoveries accelerate, we may need to censor even more genetic data. The line between digital data and our physical world is not as clear cut as it once was, with the advent of 3D printing technologies and DNA synthesisers. Many people are familiar with the first printed gun, cited heavily by the media as a dangerous development. But many would probably be surprised to learn that analogous technology is used to print pathogens. For example, the polio virus was successfully recreated in 2002, and the 1918 flu virus was resurrected by a DNA synthesiser in 2005.

Pandora's box 2.0

The machines that make this resurrection possible serve many legitimate research purposes. Instead of painstakingly manipulating DNA in a local lab, scientists can get made-to-order sequences from a variety of DNA synthesis companies from around the world. Alternatively, if they have some extra cash and desk space, they could get one of the machines right here on Ebay. Access to such a machine gives scientists a critical edge in many areas of genomics research.

But the increasing accessibility to this technology raises concerns about the "dual-use" nature of it as an unprecedented weapon. President Obama was worried enough to commission a report on the safety of synthetic biology, while volunteers have created software to detect malicious DNA sequences before an unsuspecting company prints them out.

Is ignorance bliss?

These are important first steps to more security, but they don't take us far enough. Part of the reason is due to something we call an "information hazard."

For the first time in human history, knowledge that is discovered has a reasonable chance of never being forgotten. And while this would normally be a great thing, it also creates a ratchet effect with dangerous information – once a bit of malicious code is online, the whole world can dissect and modify it.

We saw this with the infamous Stuxnet virus which appeared in 2010 – an elegantly created computer virus designed to hack Iranian nuclear labs and manipulate centrifuges to the point of breaking them. While this may have been a strategic boon for Israel and the United States, we now must contend with the availability of Stuxnet's source code, which was later posted to Github. The genius mechanisms the virus used to bypass security systems are now available to the world for delivery of alternative cyber payloads.

If a similar dynamic emerged with biological code rather than computer code, the results could be catastrophic. About a century ago, 50m people died due to a particularly lethal strain of flu, the genome of which is available online. And it is estimated that if the same virus were to be released today, the initial death toll could top 80m. Any knowledge or technology that has the capability for such destruction ought to be handled with the same caution we give to nuclear secrets, even if it means slowing the advances in medical biotechnology.

International agreements

In 2004, George Church from Harvard Medical School argued in favour of a number of US regulations in his "Synthetic Biohazard Non-Proliferation Proposal." First and foremost, he proposed that the DNA synthesis machines should be tracked and only available to licensed companies, nonprofits, or government entities. These licensed bodies should in turn be subject to strict regulations and frequent safety testing. But the stability of Church's proposal is compromised from the

difficulties of international enforcement – should any country reject these regulations, the danger still persists.

The 1972 Biological Weapons Convention, which originally codified an international agreement against the development of biological weapons, should be revamped to be fully effective. Only a multilateral approach can fully solve the regulation problem associated with synthetic biology, since viruses can spread across international borders as quickly as the airplanes carrying them.

We also need to give some serious thought to how openly we want to develop biotechnology. As Nick Bostrom, founder of the Future of Humanity Institute at Oxford University, once said:

It is said that a little knowledge is a dangerous thing. It is an open question whether more knowledge is safer. Even if our best bet is that more knowledge is on average good, we should recognise that there are numerous cases in which more knowledge makes things worse.

In the case of synthetic pathogens, our probing could indeed make things much worse if we're not careful.

Source: The Conversation