PACNET

TOMORROW'S BIOSECURITY SURPRISE

BY THOM DIXON

Thom Dixon (thom.dixon@mq.edu.au) is vice president with the Australian Institute of International Affairs NSW and a research fellow with Remi AI, an artificial intelligence company based in Australia and the US. He recently completed a non-resident WSD-Handa fellowship with the Pacific Forum that led to the publication 'Mapping the potential impact of synthetic biology on Australian foreign policy' in the Australian Journal of International Affairs.

As the biological sciences converge with the information sciences, policy makers need to be on the lookout for technological surprise. I recently happened on an old CIA memorandum declassified from 1984 and it notes how technological surprise is a type of warning failure. It says that quite often these warning failures occur not because of insufficient data, but because of fuzzy reporting and a lack of action. What's more, technology surprise is more pronounced than conventional surprise attacks because the timeline of events is prolonged, and the immediate consequences less fatal.

Enter synthetic biology, a sub-discipline of the biological sciences that when mentioned is still followed by a brief explanation of what it is, even though the discipline has been around since at least 2002. Like most scientific disciplines, the term lends itself to explanation by example, rather than by definition.

Synthetic biology is the application of engineering principles to biological systems. Or, it is the engineering of yeast so that it can ferment opioids instead of ethanol. It is the engineering of DNA so that it can store information in an energy efficient format. It is the convergence of DNA (base-4) with binary (base-2) and the treatment of genetic information like software.

My interest in this initially came from a security perspective: the synthesis of horsepox in 2017 proved what was long thought possible – that you could boot up an extinct orthopox virus through mail-order DNA parts. When the method for doing this was published in an openly accessible journal in 2018, the biosecurity community said a red line had been crossed and that the re-emergence of smallpox (horsepox's cousin) must be more actively considered.

When I started looking into synthetic biology as part of my non-resident WSD-Handa fellowship at Pacific Forum last year, I realized that synthetic biology could re-write much more in the biosecurity landscape than emerging infectious diseases. The emergence or re-emergence of infectious diseases was really just an old risk, something that dated back to the biological sciences pre-synthetic biology. Synthetic biology, by contrast, could re-write distributions of power in the international system. These security concerns were entirely novel, and sorting through fact from fiction became a necessity.

Predicting an emerging capability is a notoriously fraught activity, but a 2017 horizon-scanning exercise by transatlantic synthetic biology experts identified 20 emerging issues. They identified key for the next five years: artificial photosynthesis and carbon capture for producing biofuels; new approaches to synthetic gene drives; human genome editing; and accelerating defense agency research in biological engineering. Emerging issues in the five to ten-year bracket included the manufacturing of illegal drugs using engineered organisms, global governance impacts arising as biology becomes an information science, the intersection of information security and bio-automation, and the effects of the Nagoya Protocol on biological engineering.

The convergence of information sciences with synthetic biology is especially important. DNA is an executable file and researchers have demonstrated that a constructed DNA sample can exploit security vulnerabilities in DNA sequencing software. Hacking launched from bio-based sources is now plausible. DNA can be spoofed, it can be planted, and it can

compromise and exploit systems. DNA is a doorway into the digital world and biocyber threats are tomorrow's concern. This doorway between the worlds of the biological and the digital demands a focus specifically on the convergence of artificial intelligence (AI) with synthetic biology.

The funding and construction of genome foundries, better known as biofoundries, is occurring around the world. These synthetic biology factories take the pipette away from the scientist and replace it with a robotic arm. They are high-throughput infrastructure and they are bringing about a fundamental phase change in the scale and speed of biotechnological capability.

AI forms a core component of biofoundries because the potential arrangement of metabolic pathways within the organisms being created (to get from low-value feedstock to high-value output) occur in an almost infinite design space. This is exactly the kind of problem AI is very good at. If you want to get from A to B using cross-species traits, AI will help you lower design time.

Traditional AI security concerns are transformed when they occur in conjunction with both long-standing and novel biosecurity issues. Booting up mail-order DNA that has been designed using AI will decentralize and distribute many biosecurity risks that have traditionally occurred at the state level.

The Select Agent list in the US is unlikely to protect against DNA that remains uncharacterized, unexplored, and unknown -- material that could be dangerous if combined in the right way. AI potentially places the capability of screening for and using novel genetic traits into many more hands than before.

There are many international regimes, instruments, and organizations that look at and focus on different areas of biosecurity: the Biological Weapons Convention, UNSCR 1540, the Global International Health Security Agenda, the WHO International Health Regulations, the Convention on Biological Diversity, the subsequent Cartagena and Nagoya Protocols, the Australia Group - the list is long. Yet for all of these instruments, biotechnology has remained largely a self-regulated domain since the discovery of recombinant DNA and the Asilomar Conference in 1975.

Our reliance on academics and scientists to navigate today's novel biosecurity issues has undergone minimal change; those who make first contact with these capabilities still tend to set the rules of the self-regulatory road. To their credit they do an amazing job, working at the coalface of tomorrow's novel ethical, security, and commercial imperatives. A consortium of biofoundry operators (for example the International Gene Synthesis Consortium) may well provide the protection we need by screening customer requests for orders seeking segments of dangerous DNA like smallpox.

Yet none of these mechanisms mitigates the potential for technological surprise. The capability of CRISPR appeared and spread quickly, and it is just one example of what will continue to occur in biotechnology, especially as AI and synthetic biology become ever more entwined.

Now you might think, what is the relevance to the Pacific, to East Asia, to the US? AI and biotechnology converge in unexpected ways and one of these is US healthcare, medical, and genomic data. A report released earlier this year, *China's Biotechnology Development*, has pointed out how lax US regulations (like the Health Insurance Portability Accountability Act) constitute a national security risk, especially when compared with the European Union's General Data Protection Regulation. US medical, healthcare and genomic data is being outsourced to China for analysis. While the report focuses heavily on human health, the patterns of cross-border use and re-use for plant, animal, and human genomic data are more important than ever before. If genetic information is software, then the states that sequence, store, and manipulate that software will be making first point-of-contact with tomorrow's biosecurity concerns, they will be the agents of self-regulation. Given current trends of investment and research concentration, there is no reason to assume the next CRISPR will originate in the US, Japan, the UK, or even the EU. US-China cooperation in areas like synthetic biology is essential so that tomorrow's self-regulatory responses – regardless of which nation finds the issue first – meet

the domestic and international interests of both states alike.

Transformative platform capabilities at the intersection of the information sciences and the biological sciences will impact the security calculus of state and nonstate actors. Though the timeline of events is prolonged and the immediate consequences less fatal, that's where you will find the seeds of tomorrow's technological surprise. That's where long-term US-China cooperation is needed more now than ever.

PacNet *commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged. Click here to request a* PacNet *subscription.*