UCL JDI Special Series on COVID-19: No. 14
ISSN 2635-1625

UCL Jill Dando Institute of Security and Crime Science

# Bio-crime and COVID-19

Mariam Elgabry
DAWES Centre for Future Crime, UCL Jill Dando Institute
May 2020

## The problem

Bio-crime is the exploitation of biological tools, data, devices and systems for criminal purposes. Decreasing costs and increasing accessibility of biotechnology and biological data make this easier. In the early 2000's DNA sequencing cost $100 million and required highly specialised institutions and expertise. Today, this costs just under $200 and can be bought online. The pandemic caused by COVID-19 was not the first and unfortunately will not be the last. The global harm caused through COVID-19 provides extortion and terrorist opportunities for those able to synthesise and release new potentially catastrophic viruses or claim they can do so.

## What we know about bio-crime and how we know it

Our current knowledge of bio-crime is limited to historical evidence of bio-warfare and past biosecurity regulation such as the Biological Weapons Convention of 1972. We recently conducted a systematic review to extract all peer-reviewed studies in the academic literature that discussed forms of emerging bio-crime with a view to informing their prevention. The review showed eight potential crime harvests that were enabled by biotechnology including, cyber-bio-crime, bio-hacking and illegal gene editing. Twenty percent of the articles described attack mechanisms that involved virus engineering for malign use.

## What we think might happen in the COVID-19 pandemic

The current estimate for the global economic impact of COVID-19 is $9 trillion. Initial findings from our survey research have indicated that the pandemic and the controversies of its origin may introduce an appealing "business model" for nefarious actors, looking to cause harm at a global scale. This accords with Interpol's latest publication discussing the pandemic as an opportunity for offenders to increase or diversify their activities.

Health data are increasingly valuable and are poorly secured. During the COVID-19 pandemic, for example, opportunistic hackers have taken advantage of the Brno University Hospital (and COVID-19 testing centre) in the Czech Republic by intercepting key clinical databases and causing suspension of scheduled operations. Other hackers have tried phishing scams in the US using the names of the World Health Organisation and the US Centres for Disease Control and Prevention. We expect these kinds of attack to increase. We also expect attacks to extend towards forms of cyber-bio-crime, where integrated biotechnology is exploited through the combined means of computers/Internet and biological/biochemical material. For example, computer-controlled biological instruments may be intercepted to subvert bio-manufacturing or bio-processing systems. The UK's attempt to outsource COVID-19 testing kits from Eurofins (Luxemburg), which were found to be contaminated with the COVID-19 virus, demonstrates the potential impact of cyber-bio-crime on health.

An increase in biohacking and DIYbio projects during the pandemic can be expected. There are reports of biohackers developing solutions remotely for DIY coronavirus detection methods to be carried out at home (if infected) or at a community lab (if not infected)— using an online protocol.

## Some ideas in response

It is evident that biosecurity needs to be redefined and redesigned. We propose:

- **Cyber-biosecurity policy and standards** to strengthen preparedness to act during a pandemic
- **Experimental approach** to biosecurity by introducing "ethical hacking" for identifying and addressing risks in a timely fashion
- **"Vulnerability disclosure for laboratories"** to complement the experimental approach for early detection and management of security vulnerabilities

The following measures might be considered by practitioners:

- **Knowledge transfer:** raising awareness of biocrime risks and educating stakeholders such as the Counter Terrorism policing network is essential. In addition, as we expect biotechnology to become more widespread and widely used, frontline police officers need to be up to date on what to expect when responding (e.g. items typically found in a lab that are safe to use and what items are red flags). This would enable effective detection of biocrime that today, either goes unreported or misclassified by directing incidents to specialist groups (e.g. Forensics, Action Fraud).
- **Reporting:** for effective biocrime prevention, detection and incident tracking is necessary. Tagging crime events from front line policing and other departments (e.g. Forensics, Action Fraud) will require a combined effort of educating practitioners in categorizing incidents correctly and the public by (for example) engaging with the media to increase awareness of the risks (and expected standards). At the same time, implementing channels for the safe reporting and recording of events.
- **Intelligence gathering:** to encourage links and activity in community labs, to engage with a diversity of groups (e.g. biohackers and hackers) while enhancing communication channels of findings (both positive and negative) and responsible research and innovation.
- **Supply chain controls:** to re-assess (and where needed to restructure) current biotechnology supply chains and apply controls of testing for imported and approved products to check on product quality and suppliers. Incorporation of supply chain tracking and managements systems could assist. Introduction of licenses and registrations of purchased kits may also assist.
- **Cyber hygiene:** needs to be implemented (e.g. Cyber-essentials in the UK) to make sure data are well secured. To address cyber-bio-security, biotechnology *systems* generating health data need be compliant to cybersecurity standards, which until today NHS trusts fail to pass cyber security assessments, even after the WannaCry ransomware attack.

**Relevant resources**

Yetisen (2018). Biohacking. *Elsevier*.
DDCMS. (2018). *Code of Practice for Consumer IoT Security*.
https://www.gov.uk/government/publications/secure-by- design
Elgabry, M., Nesbeth, D., & Johnson, S. D. (2020). A systematic review protocol for crime trends facilitated by synthetic biology. *Systematic Reviews*, *9*(1), 22. https://doi.org/10.1186/s13643-020-1284-1
Gradoń, K. (2020). Crime In The Time Of The Plague: Fake News Pandemic And The Challenges To Law-Enforcement And Intelligence Community. *Society Register*, *4*(2), 133–148.
Peccoud, J., & Murch, R. (2017). Cyberbiosecurity: From Naive Trust to Risk Awareness Cyberbiosecurity: Securing the Emerging Domain of Biomanufacturing *Trends in Biotechnology*

*This is one of a series of short, speculative papers developed by the UCL Jill Dando Institute during the current pandemic. It is edited by Nick Tilley and Gloria Laycock and published by University College London. The raison d'être of the series is fully described at: https://www.ucl.ac.uk/jill-dando-institute/research/covid-19-special-papers*