Written evidence submitted by Mariam Elgabry[1,2]

1. DAWES Centre for Future Crime, Jill Dando Institute for Security and Crime Science, University College London
2. Advanced Centre for Biochemical Engineering, University College London

I am a PhD researcher at University College London, where I have a joint appointment in the Department of Security and Crime Science and the Advanced Centre for Biochemical Engineering (ACBE), specifically in Synthetic biology. I am supervised by Dr. Darren Nesbeth, associate professor in synthetic biology at UCL Biochemical Engineering and Professor Shane Johnson, director of the Dawes Centre for Future Crime at UCL, which conducts research into future crime threats and how we might respond to them. Both supervisors work regularly with industrial partners, Dr. Nesbeth has previously advised the City of London on biotechnology and Internet companies on financial communication strategy as they sought initial public offering (IPO) on UK and European equity markets.

My background is in Biochemistry and mathematical modelling of biological systems and I have industrial experience in the pharmaceutical, technology and security design industries. During my time at AstraZeneca Pharmaceuticals, I received the Linda Eteen Memorial Best Performance Prize (2015) for building an early detection system within the drug development pipeline. I received my MSc in Bioinformatics from Imperial College London in 2016 and worked for Microsoft as a Partner Lead on teams of 25+ (Imperial and UCL) where I was invited to represent the UK from over 2800 candidates at Microsoft HQ (Seattle). After receiving my MRes in Security and Crime science I consulted in security design for a year developing tools to automate crime risk assessments and analyses of neighborhoods in London. I am also co-founder and CTO of Enteromics Ltd. (12188084), a medical technology start-up with a mission to unlock the gut microbiome for sustainable healthcare by building a secure IoT pill and platform.

Having worked in industries that combine deep-tech expertise with biochemical wet-lab experience, I submitted a research proposal in 2016 and was awarded a DAWES-EPSRC funded PhD studentship to conduct my current research that focuses on Biocrime and Cyber-biosecurity at UCL. This research aims to inform, influence and underpin evidence-based policymaking in the UK regarding synthetic biology and, where relevant, to change organisational culture and practices to improve national security.

My submission is focused on the following three areas:

- *The main drivers of biosecurity risks to human health in the UK, including pandemics and emerging infectious diseases;*
- *How, and how effectively, these risks are monitored and assessed by the UK Government, and by whom; and whether the specific type of risk to the UK represented by Covid-19 fell within such monitoring and assessment processes;*
- *Domestic preparedness and the extent to which the Government's planning for pandemics in the 2018 Biosecurity Strategy helped in guiding that preparedness.*

Executive Summary

- The main drivers for deliberate biosecurity threats in the form of biocrime are rapidly evolving

- Synthetic biology and related biotechnological developments are becoming more integrated and inter-connected, facilitating crime and biosecurity risks
- There is an urgent need and opportunity for the UK to support its growing bioeconomy by developing effective biocrime prevention mechanisms against modern biological threats
- Through a systematic review and Delphi study conducted between April 2019 – May 2020 at the University College London, the inquiry topics were considered in detail and three key recommendations emerged:
    1. Create **Cyber-biosecurity policy, standards and liaison** to strengthen preparedness to act to biosecurity risks to human health, including from pandemics;
    2. **Adopt an experimental approach** to biosecurity by introducing "ethical hacking" in all sectors for identifying and addressing risks as a harm reduction tactic;
    3. **"Vulnerability disclosure for laboratories"** to complement the experimental approach for early detection and management of security vulnerabilities across all sectors;

Background

To understand the current landscape, we developed a systematic review protocol [1] as a methodology to identify and synthesise current evidence on biocrime. The review was then conducted between April - August 2019 and was designed to provide a complete and exhaustive summary of the current evidence in the academic literature that is relevant to crimes facilitated by synthetic biology with a view to informing their prevention. We found 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. The systematic review, currently under review, is available on request.

To compliment the systematic review, we conducted a parallel Delphi study with two participant groups [2] between September 2019 and May 2020 on the future of biocrime for biosecurity and health policy implications in the UK. In addition to interviewing traditional experts in national intelligence and security services, we interviewed non-traditional experts, given their unconventional technical expertise. We asked for their opinions on emerging biocrime trends facilitated by synthetic biology and what, if anything, should be done to safeguard against it. Non-traditional experts included "biohackers", a largely hidden population, and consisted of highly technical individuals that practice synthetic biology outside formal institutions that may or may not have had formal scientific training. Having two groups and using the opinions of recognized and "non-traditional" experts was an advantage as crimes are expected to be more sophisticated in the future; which as illustrated with the current COVID-19 pandemic, governments may be ill-prepared to meet and that may have not yet begun to address.

I have contributed to the Jill Dando Institute of Security and Crime science series of special papers as a response to the COVID-19 pandemic that focuses on the implications of Bio-crime and the COVID-19 pandemic for police agencies and other organisations, available here [3].

A summary of the main outcomes from my research that relate to the seven inquiry topics is presented below, followed by key recommendations that we propose in response.

Inquiry Topics

- Biosecurity Risks

There are distinctions to the main drivers behind natural, accidental and deliberate biological threats. Our work focuses on **deliberate** biosecurity threats in the form of biocrime. Bio-crime is the exploitation of biological material, tools, data, devices and systems for criminal purposes. We identify three main drivers of biocrime.

(1) decreasing costs and increasing accessibility of biotechnology enabling biohacking and illegal gene editing. For instance, genetic engineering technology that was once limited to highly specialised institutions and expertise, is now available in kits that can be purchased online. There are reports of biohackers and autologous gene therapies or unregulated gene therapy CRISPR/Cas constructs developed "at-home" and tested through "self-experimentation" and self-injection [4]. Moreover, twenty percent of the articles screened in the systematic review described attack mechanisms that involved virus engineering for malign use.

(2) increasing availability of biological and health data and increased hyper-connectivity / hyper-personalisation in healthcare and medicine increasing the attack surface for crime. Recent examples of targeted and/or exploited health data in the UK include the NHS WannaCry ransomware attack (2017) [5], UK Forensic processing unit attack (Eurofins) [6] and 100,000 Genomes Project and NHS hack (2018) [7]. Moreover, there exists a global mega-trend of consumer-centric technology — the Internet of Medical Things (IoMT) — as consumers are increasingly health-conscious and seek health information from resources other than their GP [8]. If the IoMT is as insecure as the internet of things (for a review, see Johnson & Blythe, 2019 [9]), this is serious concern.

(3) increasingly integrated and inter-connected biotechnology systems, supply chains and workflows. This enables cyber-biocrime, where integrated biotechnology is exploited through the combination of computers/Internet and biological/biochemical material [10]. For instance, the sound produced by DNA synthesizer machines during sequence synthesis can be exploited to enable the theft of propriety (and potential dangerous) data (e.g. sequence of a highly contagious virus) [11]. This introduces a plausible business model for malicious actors as it has been demonstrated with over 80% accuracy, taking only 56 hours and $300 to achieve. Other research suggests that a target computer system can be compromised using malware stored in physical DNA [12].

- Risk Monitoring and Assessment Processes

Although not a biocrime, the COVID-19 pandemic illustrates the impact that a potential deliberate biosecurity threat could have. The UK Government's response can be evaluated using three main examples.

(1) The current estimate for the global economic impact of COVID-19 is $9 trillion [13]. Initial findings from our Delphi study 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 [14].

(2) Health data are increasingly valuable but often poorly secured. For example, during the COVID-19 pandemic, hackers of Hostile states have been reported by UK cybersecurity agencies to target British universities and scientific facilities working on vaccine development [15]. Initial findings from our Delphi interviews indicate that universities and the research generated in academic settings may become a crime hotspot, which may be important in the follow up UK Government's 'Integrated Security, Defence & Foreign Policy Review'.

(3) Cyber-biosecurity and related supply chains must be reevaluated. 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 [16].

- Domestic Preparedness and the 2018 Biosecurity Strategy

Continued evidence from my research indicates that biosecurity is outdated and often outpaced by emerging and converging technology. The 2018 Biosecurity Strategy, for example, does not cover the cyber-biosecurity risks highlighted here.

With a UK bioeconomy and the upcoming British exit from the European Union, biosecurity and its risks to human health need to be addressed in future UK policy and governance. This will require cross-government efforts. For instance, it is expected that the Internet of Medical Things (IoMT) or medical devices (currently regulated by the Medicines and Healthcare products Regulatory Agency (MHRA) and notified bodies) will move into consumer-focused products and may require a collaborative and comprehensive risk mapping between MHRA and the Department for Digital, Culture, Media & Sport (DCMS). Existing EU regulations of medical devices may provide an opportunity for the UK to redefine such measures and in doing so strengthen the development of devices with security built-in at the design stage.

It may be wise to increase communication channels between advanced technology stakeholders and parliament through All-party parliamentary groups (APPG). There is currently an APPG on Medicines and Medical Devices and one in Cybersecurity. However, there is no APPG to cover IoT/ IoMT or Cyber-biosecurity risks, which relate to the

integration, inter-relation and user-interaction of technologies; as opposed to the evaluation of a technology in a silo.

Three Key Recommendations

Biotechnology increasingly contributes to the global economy; however, it introduces new attack vectors that surpass the current biosecurity paradigm of shortlisted pathogens. The outcomes of the systematic review and initial findings from the Delphi study highlight the following key recommendations that can help promote the objectives of the UK Biological Security Strategy.

1. **Create Cyber-biosecurity policy, standards and a governing body** to strengthen preparedness to proactively (and if that fails, reactively) reduce the risks associated with biosecurity risks to human health, including from pandemics;

In order to do so, four main mechanisms are proposed in relation to the UK's supply chains, biosecurity risk assessment and overall security, as follows:

(i) **supply chains** and integrated systems of biotechnology (and related) need to be reexamined and re-assessed (and where needed restructured) to apply controls of testing for quality and security. Incorporation of supply chain tracking and management systems could assist. Introduction of licenses and registrations of purchased supplies may also assist.

(ii) **cyber hygiene** needs to be extensively implemented (e.g. Cyberessentials in the UK) to make sure data are well secured. To address cyber-biosecurity, biotechnology systems generating health data need be compliant with cybersecurity standards. As of today, we understand that some NHS trusts still fail to pass cyber security assessments, despite the gravity of the WannaCry ransomware attack [17].

(iii) **research activity** is important to the economy but should be assessed in terms of its security implications. This does not need to be alarmist. Researchers are currently required to consider the ethical implications of their research, but a consideration of the crime and security implications of it is not an explicit requirement. Such a consideration could be included as an element of responsible research and innovation and a condition of funding for research councils (and other related bodies).

(4) creating a **National Centre for Biosecurity and Biosafety** may strengthen preparedness whilst driving a positive change in culture towards improved cyber-bio-hygiene, as suggested by [18].

2. **Adopt an Experimental approach** to biosecurity by introducing "ethical hacking" for identifying and addressing risks;

Ethical hacking is the proactive (and authorized) act of bypassing a system's security to identify potential threats and vulnerabilities that could be exploited by malicious hackers [19]. This approach is adopted by businesses to protect digital infrastructure. In the case of biosecurity, we propose that efforts should be made to move away from the implementation of reactive changes after major events occur, to proactive governance in health security and

biosecurity. The introduction of ethical hacking across all sectors — industry, academia, government, and especially the third sector, such as community laboratories — is one approach that could contribute to a more proactive approach. The 2018 Biosecurity Strategy does not specifically cover community laboratories and "hackspaces" that, while bringing substantial positive benefits by enabling national experimental innovation and local technical upskilling, can enable **enhanced vulnerability management** (the iterative process of identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities) [20].

Biosecurity risks need to be mapped consistently and more exhaustively. In doing so, we suggest that government and similar bodies should consult with a **diverse group of stakeholders** to include biohackers and hackers.

3. **"Vulnerability disclosure for laboratories"** to complement the experimental approach for early detection and management of security vulnerabilities across all sectors;

In addition to government working more closely with academia, strengthening communication with the biohacking community can act as a harm reduction tactic. This model is successfully adopted by the US, where the FBI engages directly with biohackers through community laboratories and sponsor synthetic biology conferences [21]. Currently, there is no clear communication channel, reporting system or engagement pathway with the biohacker community in the UK. We would encourage government or their representatives to form active links with community labs, to engage with a diversity of groups (e.g. biohackers and hackers) and to enhance communication channels of findings (both positive and negative) and responsible research and innovation. This will need to be done carefully and should take on board findings from behavioral science and other fields to increase the likelihood of engagement.

The 2018 Biosecurity Strategy describes a point of contact for research that may introduce dual-use applications, however, as yet there is no central governmental entity appointed. It is necessary to implement both formal and informal channels for the safe **reporting and recording** of events for effective biocrime prevention, detection and incident tracking. This will ensure monitoring occurs and that relevant actions are taken.

17 June 2020

References

[1] Elgabry, M., Nesbeth, D. & Johnson, S.D. A systematic review protocol for crime trends facilitated by synthetic biology. Syst Rev 9, 22 (2020). https://doi.org/10.1186/s13643-020-1284-1 Available here

[2] Linstone, H. and Turoff, M. (editors) (1975) The Delphi Method: Techniques and Applications, Addison Wesley Advanced Book Program.

[3] Elgabry, M. (2020) Bio-crime and COVID-19, UCL JILL DANDO INSTITUTE OF SECURITY AND CRIME SCIENCE - COVID-19 Special papers Available here

[4] Kirkpatrick, J., Koblentz, G.D., Palmer, M.J., Perello, E., Relman, D.A. and Denton, S.W. (2018) Editing Biosecurity: Needs and Strategies for Governing Genome Editing. George Mason University.

[5] Clarke, R. and Youngstein, T., 2017. Cyberattack on Britain's National Health Service—a wake-up call for modern medicine. N Engl J Med, 377(5), pp.409-11.

[6] Muncaster, P. (2019) Eurofins Ransomware Attack Led to Backlog of 20,000 Cases, Infosecurity (2019) (March 26, 2020).

[7] Teiss (2018) "Hackers Mounting Cyber-Attacks to Access DNA Data of Thousands of Brits." www.teiss.co.uk/hackers-dna-data-brits/.

[8] Joyia, G.J., Liaqat, R.M., Farooq, A. and Rehman, S., (2017) Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain. J Commun, 12(4), pp.240-7.

[9] Blythe, J.M. and Johnson, S.D., 2019. A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, pp.1-29.

[10] Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G. and Raman, S., 2018. Cyberbiosecurity: from naive trust to risk awareness. Trends in biotechnology, 36(1), pp.4-7.

[11] Faezi, S., Chhetri, S.R., Malawade, A.V., Chaput, J.C., Grover, W.H., Brisk, P. and Al Faruque, M.A., (2019) January. Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines. In NDSS.

[12] Ney, P., Koscher, K., Organick, L., Ceze, L. and Kohno, T., 2017. Computer Security, Privacy, and {DNA} Sequencing: Compromising Computers with Synthesized {DNA}, Privacy Leaks, and More. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 765-779).

[13] G. Gopinath (2020) The Great Lockdown: Worst Economic Downturn Since the Great Depression. IMF (April 28, 2020). https://blogs.imf.org/2020/04/14/the-great-lockdown-worst-economic-downturn-since-the-great-depression/

[14] INTERPOL (2020) INTERPOL assisting member countries to mitigate and investigate attacks against hospitals, Available at: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[15] Grierson, J., and Devlin, H. (2020) "Hostile States Trying to Steal Coronavirus Research, Says UK Agency." *The Guardian*, Guardian News and Media, 3 May 2020, www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency.

[16] Evening Standard, (2020) "Coronavirus Tests Heading to UK Contaminated with Covid-19." www.standard.co.uk/news/health/coronavirus-test-kits-contaminated-covid-19-a4403021.html.

[17] Syal, R. (2018, February 5). *Every NHS trust tested for cybersecurity has failed, officials admit*. The Guardian. https://www.theguardian.com/technology/2018/feb/05/every-nhs-trust-tested-for-cyber-security-has-failed-officials-admit

[18] Nelson, C., Bonsall, Thompson, R. et al. (2019) UK Government's approach to emerging infectious diseases and bioweapons, Future of Humanity Institute Oxford, Availabe here

[19] Pashel (2007) Teaching students to hack: Ethical implications in teaching students to hack at the university level in Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD ’06, (2007), pp. 197–200.

[20] Foreman, P (2010): Vulnerability Management, pg 1. Taylor & Francis Group.

[21] Wolinsky, H. (2016). The FBI and biohackers: an unusual relationship. *EMBO Reports*, *17*(6), 793–796. https://doi.org/10.15252/embr.201642483