Written evidence submitted: 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 research bio-crime and Cyber-biosecurity with the aim to inform, influence and underpin evidence-based policymaking in the UK and, where relevant, to change organisational culture and practices to improve national security. 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 external stakeholders, Prof Shane with (for example) the Home Office and UK police forces and and Dr. Nesbeth has previously worked with citizen science groups such as the London BioHackspace.

Alongside my research, I am co-founder and Director of Enteromics Ltd. (12188084), a medical technology start-up, supported by Innovate UK, that builds secure gut-sensing pills, and was in the Top 5 start-ups in last year's Mayor's Entrepreneur Health Award, hosted by Sadiq Khan, Mayor of London.

My background is in deep-tech and bioengineering and I have industrial experience from leading award-winning projects during my time at Astra Zeneca and Microsoft. My work has been published by the UK Parliament Joint Committee on National Security [1], presented my work to the Home Office and 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 organizations, available here [2] featured in Policing Insights. I have also been shortlisted as Greek International Woman of the year (2021) under Science and Technology.

Having submitted evidence in the previous inquiry to the UK Joint Committee for National security and biosecurity, I submit further evidence to support our key recommendations of creating UK cyber biosecurity policy and adapting an experimental approach through a proposed “Hybrid Hackathon Delphi Model” that I am currently conducting.

My submission is focused on the following inquiry area:

- how ‘red-teaming’ might be introduced into national security decision-making;

Executive Summary

- In an increasingly health-centred global economy, there is an urgent need and opportunity for the UK National security machinery to support its digital biosecurity.
- The hackathon model is an efficient way to produce functional prototype applications
- A 2020 Delphi study we conducted involved “non-traditional” experts such as “biohackers” to forecast biocrime trends and operated an effective “red teaming” exercise
- We propose a Hybrid Hackathon Delphi Model (HHDM) as a ‘red-teaming’ approach that can be introduced into national security decision-making
• HHDM captures current and nuanced opinions of diverse field experts while also generating detailed hacking proposals

Background

In our previous submission we considered the inquiry topics through overviewsing a systematic review [3, 4] and Delphi study conducted between April 2019 – May 2020 at the University College London, and we provided three key recommendations for biosecurity and national security planning and resilience implementation:

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. Increase **biotechnology and biosecurity literacy** to complement the experimental approach for early detection and management of security vulnerabilities across all sectors;

Since then and to demonstrate these three key recommendations, I am leading the very first Internet-of-Ingestible-Things™ workshop supported by the Dawes Centre for Future Crime. By collaborating with Enteromics, a UK MedTech startup that builds ingestible medical devices, and the Biohacking Village (BHV), a non-profit organization (83-3941479) focused on healthcare security, we aim to develop a “proof of concept” red-teaming approach that can be introduced to aid national security decision-making while using ingestible medical devices as an example technology and testbed.

The Internet-of- Ingestible -Things™ (IoIIT) are smart gut-sensing pills or internet-connected ingestible medical devices used to monitor gastrointestinal health. Medical devices are products (instrument, apparatus, machine, implant, software or related article) intended to be used for the specific medical purpose(s) of diagnosis, prevention, monitoring, treatment or alleviation of disease (WHO). In Healthcare, it is vital to ensure that internet-connected ingestible medical devices are secure as these collect sensitive information about the patient. For an insecure device, a key concern would be that it could cause direct harm by interfering with health outcomes. For example, Applegate (2013) exposed a vulnerability in a pacemaker that gave unauthorized access and control to the device such as the ability to deliver an unwarranted shock through a pacemaker via wireless transmission [5]. Li et al (2011) disclosed vulnerabilities found in insulin pumps used to deliver regular insulin throughout the day. They were able to alter the intended therapy which could overdose the patient remotely [6]. The current medical device regulatory framework is limited to a security risk assessment and guidance, as opposed to active security testing, and requires more (specialized) auditing.

In contrast to what has been traditionally the case for the development of medical devices, where security is applied retrospectively as a compliance check, here we proactively think about security at the design stage of the product lifecycle to safeguard against malicious misuse. Using a parallel Delphi and “hackathon” model we engage with non-traditional experts such as ethical hackers (authorized testers of a target systems’ security to report any found weakness or
vulnerabilities with the aim to develop instruction for their remedy [7]. The Internet-of-Ingestible -Things™ workshop aims to inform good practice by delivering a set of principles through a policy briefing for cyber biosecurity to prioritize responsible health tech for a more “bio-savvy” public - essential, now more than ever, as devices flood the market in response to COVID-19, that has highlighted weakness in an overburdened healthcare system and in cyber-biosecurity supply chains.

We propose that this – or a similar model – be introduced to national security as a continuous cycle of inquiry in emerging technology to challenge assumptions, crowdsource ideas and coins of collective intelligence through speculative design and scenario building exercises with the aim to proactively identify early warnings and integrate elicited opinions that can aid decision making to safeguard against potential national security threats.

A summary is presented below of the methodology for the proposed “Hybrid Hackathon Delphi Model” as a ‘red-teaming’ approach that relates to the inquiry topic.

**Inquiry Topic**

- how ‘red-teaming’ might be introduced into national security decision-making;

Red teaming or ethical hacking is the authorized testing of a target systems’ security to report any found weakness or vulnerabilities with the aim to develop instruction for their remedy [7].

The Internet-of-Ingestible-Things™ workshop will demonstrate a proof-of-concept model to systematise the “hackathon” model. The “hackathon” model dates back to the 1960’s where Massachusetts Institute of Technology (MIT) students gathered to 24-hr computer program coding “sprints”[8], later popularized in the Information Technology (IT) community in the form of contests with prizes to produce functional prototype applications and in doing so accelerating innovation.

**Our 2020 Delphi study**

The Delphi protocol [9] is a technique originally developed for the purposes of horizon scanning - to determine the consensus of a group of experts on a given complex problem. In our previous 2020 Delphi study (under review and available upon request) we had two group of experts: one group of “traditional” field experts, such as government officials, researchers, or industry professionals, and another group of “non-traditional” experts, such as “biohackers” (an individual who has technical experience in either innovating, developing or using biotechnologies, with or without professional or academic qualification), entrepreneurs, early-adopters of technology, and technicians.

Our 2020 Delphi forecasted crime trends facilitated by commercialized biotechnology to address the inquiry of what might biotechnology crimes look like in the next five years.

The outcomes of which have informed the construction of this subsequent Delphi study with a focus on ingestible devices as an emerging technology and to forecast the direction and form of security required. We combine the parallel Delphi methodology but implement a “hackathon” model for the recruitment of participants and introduce a new (third) participatory group.
We propose this Hybrid Hackathon Delphi Model as ‘red-teaming’ approach that can be introduced into national security decision-making.

**Hybrid Hackathon Delphi Model**

The Implementation plan of the Hybrid Hackathon Delphi Model constitutes a three-month format, with three stages. The first stage comprises of contextual talks inviting stakeholders (an individual, group, or organization, who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project" [10]) at the forefront of their field to share prospects and challenges of the technology under investigation. The second stage invites stakeholders of the industries of interest to form “cross pollinated” teams and undergo a workshop with the aim of interest. Finally, the teams’ proposals are shared with both a judging panel comprising of specialist profession but also to the public to deliver relevant policy briefing.

Using the IoT as an example application of the Hybrid Hackathon Delphi Model, the aim of this project is to illicit opinions from field experts on a security-by-design framework relevant to the Internet-of-Ingestible-Things™. We recruited ten stakeholders from a mixture of industry, academia and government to speak during the first phase. Speakers included leaders of cyber-biosecurity and future crime research, cybersecurity professionals, medical device manufacturers but also users of the IoT devices such as patients and clinicians. The talks were one hour sessions published, promoted and publicly available via social media channels (e.g., LinkedIn, Youtube, Twitter) and overviewed cutting edge research and practice related to Cyber biosecurity, biocrime, future crime, consumer market readiness for ingestible devices, and the gut microbiome.

We also recruited three judges with specialist professional backgrounds in medical devices, cyber security by design and security engineering with a focus on network exploitation and IoT.

Participants were recruited via communities, worldwide. We reached ethical hackers from hacking conventions (e.g. DEFCON), organizations (e.g. BHV), community labs (e.g. BioHackspace London, Frugal scientists), academia (e.g., UCL) and industry (e.g. Microsoft). We reached policy and regulatory practitioners through the Dawes Centre for Future Crime, which has a database of over 700 practitioners (e.g. MHRA, BSI, GO, DSTL). We reached the medical device network through the Institute of Health Engineering and Enteromics ltd. (e.g., CPI). Finally we reached patient groups through communities and societies (e.g., Hellenic society, Girls with Guts).

Interested participants applied through an online form open to all and available online. The form contained questions that helped allocate interested participants in “cross-pollinated” teams (technical, policy maker e.t.c.). To apply, teams were asked to ideate an ingestible things device design, assess and identify an application with a focus on designing security in. Seven groups of four team members each applied to the hackathon and submitted their designs.

Applicants undergo a selection process to identify the top three teams that will progress to the next stage of four one hour one-to-one workshops from specialists in production manufacturing and design, digital biosecurity and ingestible device developers to prototype their ingestible things device designs.
Before prototyping, team members undergo a parallel Delphi process that informs potential policy requirements for ingestible devices but that in itself too, informs the teams’ designs within the hackathon. In this Delphi study we had an additional group of patients (e.g., Inflammatory Bowel Disease, Irritable Bowel Syndrome) given the technology being assessed as end-users of the devices, their input in security design is vital. Each group will complete three survey rounds (May 2021): the first round involves structured interviews, whereby 6 “open” questions are asked related to ingestible device security and how best to implement this. In the second round, participants will be sent a survey (an online electronic form) with the same questions as the first round, but with choices derived from the responses of the participants from the first round. In this round, participants will be asked to review the responses and rate each of them on a seven-point scale (Strongly agree, Agree, Moderately agree, Uncertain, Moderately disagree, Disagree, Strongly disagree). Finally, the third round will consist of the consensus phase, whereby responses are examined by participants according to the majority agreement/disagreement.

The aim is to provide consensus and establish priorities with regards to the factors that promote security design implementation and continued development of ingestible medical devices from patients, medical device manufacturers/regulators and biohackers.

Following the workshop phase, a two-minute video demonstrating their designs is expected from the teams (first two weeks of June 2021) that will be assessed by field experts that constitute the judging panel but also the public shared via social media channels – as to address the third recommendation of increasing public biotechnology and biosecurity literacy.

**Introducing the Hybrid Hackathon Delphi Model in National Security Machinery**

In an increasingly health-centered global economy, there is an urgent need and opportunity for the UK National security machinery to support its digital biosecurity. Because of the concerns highlighted in the recent UK Biosecurity and national security report to which we have contributed to, there is an urgency in the need to establish effective national security structures to prepare for future emergencies.

As biotechnology increasingly integrates into the global economy, it introduces new attack vectors that surpass the current national security structures. The hackathon model is an efficient way to produce functional prototype applications and our 2020 Delphi that involved “non-traditional” experts such as “biohackers” proved an effective “red teaming” exercise to forecast biocrime trends.

National security decision-making deals with uncertainty and limited evidence. The Hybrid Hackathon Delphi Model captures current and nuanced opinions of diverse field experts while also generating detailed hacking proposals. In doing so, the HHDM introduces cognitive and background diversity for better decisions, innovation and implementation, for better public trust.

**Conclusion**

We propose this Hybrid Hackathon Delphi Model as ‘red-teaming’ approach that can be introduced into national security decision-making. We propose that this – or a similar model – be introduced to national security as a continuous cycle of inquiry in emerging technology to challenge assumptions, crowdsource ideas and coins of collective intelligence through
speculative design and scenario building exercises with the aim to proactively identify early warnings and integrate elicited opinions that can aid decision making to safeguard against potential national security threats.

30 April 2021

References


