Futures 141 (2022) 102970

Contents lists available at ScienceDirect

Futures

journal homepage: www.elsevier.com/locate/futures

# The future of biotechnology crime: A parallel Delphi study with non-traditional experts

Mariam Elgabry [a,b,*], Darren Nesbeth [b], Shane Johnson [a]

[a] DAWES Center for Future Crime at UCL, Jill Dando Institute for Security and Crime Science, 35 Tavistock Square, London WC1H 9EZ, United Kingdom
[b] UCL Biochemical Engineering, Bernard Katz, London WC1E 6BT, United Kingdom

ARTICLE INFO

*Keywords:*
Delphi
Synthetic biology
Crime
Biotechnology
Futures
Biohackers

ABSTRACT

*Background:* The way science is practiced is changing and forecasting biotechnology crime trends remains a challenge as future misuses become more sophisticated.
*Methods:* A parallel Delphi study was conducted to elicit future biotechnology scenarios from two groups of experts. Traditional experts, such as professionals in national security/intelligence, were interviewed. They were asked to forecast emerging crime trends facilitated by biotechnology and what should be done to safeguard against them. Non-traditional experts, such as "biohackers" who experiment with biotechnology in unexpected ways, were also interviewed. The study entailed three rounds to obtain consensus on (i) biotechnology misuse anticipated and (ii) potential prevention strategies expected.
*Results:* Traditional and non-traditional experts strongly agreed that misuse is anticipated within the cyber-infrastructure of, for example, medical devices and hospitals, through breaches and corporate espionage. Preventative steps that both groups strongly advocated involved increasing public biosecurity literacy, and funding towards addressing biotechnology security. Both groups agreed that the responsibility for mitigation includes government bodies. Non-traditional experts generated more scenarios and had a greater diversity of views.
*Discussion:* A systematic, anonymous and independent interaction with a diverse panel of experts provided meaningful insights for anticipating emerging trends in biotechnology crime. A multi-sector intervention strategy is proposed.

## 1. Introduction

The way science is practiced is changing and this is as true for biotechnology as it is for other sciences. For example, Life science is ever more integrated within the cyber-domain as laboratories become "connected" and scientific research is increasingly dependent on internet-connected systems, tools and devices (Peccoud et al., 2018). Broader community groups also work in the biotechnology space due to declining costs of technology and the increasing accessibility of community facilities (Nieuwenweg et al., 2021). Synthetic biology is the engineering science of redesigning organisms for useful purposes by modifying them to have new abilities (Agapakis,

*Abbreviations:* NASEM, National Academies of Science, Engineering and Medicine; T, Traditional experts; NT, Non-Traditional experts.

* Corresponding author at: DAWES Center for Future Crime at UCL, Jill Dando Institute for Security and Crime Science, 35 Tavistock Square, London WC1H 9EZ, United Kingdom.
*E-mail address:* M.elgabry.17@ucl.ac.uk (M. Elgabry).

https://doi.org/10.1016/j.futures.2022.102970
Received 20 December 2021; Received in revised form 5 April 2022; Accepted 26 May 2022
Available online 6 June 2022

2014); in the same way that computers can be re-programmed for specific functions. For example, the immune cells of patients can be engineered to recognise and attack cancer cells, so-called CAR (for chimeric antigen receptor) technology (June et al., 2018). Once beyond the reach of those without significant experience and technical expertise, synthetic biology is now practiced outside of the regulated institutional premise and – when it is – is referred to as biohacking. The term "hacking" here has a positive meaning and is defined as the "finding [of] unintended or overlooked uses" and "applying them in new and inventive ways to solve a problem – whatever it might be" (Erickson, 2008, p. 1). Biohackers' activities involve, for example, the development of genetically engineered compounds (e.g., *N6* gene to produce HIV antibodies, and the *myostatin* gene for muscle growth) that they have experimentally produced on their own using gene editing technology such as CRISPR/ Cas 9 (Ran et al., 2013) —and tested through self-experimentation (Kirkpatrick et al., 2018). Biohackers have been previously reported to reverse engineer patented gene therapies (Kirkpatrick et al., 2018), and more recently to be investigating the potential of (free and Open) vaccines against the SARS-CoV-2 global pandemic (Heidt, 2020; Brown, 2020; Accademia Nazionale dei Lincei, 2020).

### 1.1. Background in biotechnology developments and the responses to them

While the development and application of biotechnology is being pursued for beneficial purposes, the pace at which it is accelerating prompts concerns about potential misuses, particularly as security is often overlooked when new goods and service are introduced (Pease, 1997). For example, the US National Academies of Science, Engineering and Medicine (NASEM) have been at the forefront of a resilience strategy against this threat landscape. NASEM developed a framework (NASEM, 2017) for identifying and assessing synthetic biology threats for the larger objective of "Safeguarding the Bioeconomy" (NASEM, 2014, 2015) of the U.S. Department of Defense. Threats of the highest concern identified included the re-creation of known pathogenic viruses (NASEM, 2018), and emerging opportunities for misuse that increased internet connectivity facilitates. The outcomes of these pivotal workshops shaped a newly defined discipline of cyber-biosecurity, which aims to safeguard valuable biological information and material between the cyber-physical domain (Murch et al., 2018; Peccoud et al., 2018). In a recent study, Elgabry et al. (2020a) systematically surveyed research concerned with the crime implications of biotechnology. The findings of that study also highlighted threats at the intersection of the bio- and cyber-domains, and the absence of frameworks in place to address them. The outcome of the systematic review highlighted the need for a cyber-bio-infrastructure in the context of crime prevention. Absent this, the study indicated that there is a very real risk of a "crime harvest" (emerging crime opportunities) occurring due to overlooked security implications (Pease, 1997). While the review was systematic, the findings were constrained to published academic research, which was found to be both scarce and fragmented. For example, of the 794 articles initially identified as being of potential relevance, only 15 ultimately met the inclusion criteria. That is, that studies explicitly made a link between biotechnology, synthetic biology, or genetic engineering and technological misuse (by discussing or demonstrating threat/attack models). The review also highlighted the fact that to date research and opinion —as found in the academic literature — has been limited to academics from the life sciences or computer science (Elgabry et al., 2020a).

### 1.2. Problem motivation

Forecasting crime trends remains a challenge, yet the way we forecast the misuse of technology has seen little evolution over time. In particular, the discussion of security implications is limited to siloed expertise from traditional professions and there has been no engagement with wider communities. For example, the committee that assessed synthetic biology threats from the NASEM report were all established individuals and/or bodies in "traditional" professions from large institutions (National Defense University), or corporations (e.g. Ginkgo Bioworks Inc.). The scale of identified and predicted biotechnology misuse is unknown and is expected to be more sophisticated in the future (Mueller, 2021). It would thus be valuable to gather information from a wider selection of experts who include those who experiment with these types of technologies in unexpected ways (Lentzos et al., 2020).

To that end, and absent a more developed literature, we conducted a Delphi study (Dalkey & Helmer, 1963; Turoff, 1970; Linstone & Turoff, 1975) to elicit opinions on emerging crime trends that may be facilitated by biotechnology. We use biotechnology as a broad term to include – but not be limited to – specific subsets such as synthetic biology as well as any emerging cyber-biosecurity issues. The Delphi methodology is useful for the prediction of the occurrence of future events where empirical data is limited or lacking; either because the event has not yet occurred or remains under-reported, unreported or unknown. In such cases, expert input is necessary (Rowe & Wright, 1996a, 1996b). A key feature of the Delphi method is that because participants provide their responses in isolation and anonymously it avoids "*group think*" (Rowe & Wright, 1999), whereby group dynamics distort the actual views of participants, and it prevents otherwise vocal participants from biasing the reported views of others (Dalkey et al., 1972). This problem is recognised by researchers and professionals alike, with the Director of the UK's MI6, recently highlighting the "danger of group think" (Butler, Review of Intelligence).

### 1.3. Contribution of this study

We conduct a Delphi study but with two groups (Coutorie, 1995). The two groups were surveyed in parallel, which allowed for the identification of differences across groups as well as the development of a picture of the potential overall threat (and solution) landscape. The first group were "traditional" field experts, such as government officials, academic researchers, or industry professionals, recruited through stakeholder mapping (see Methods section). The second (parallel) group consisted of "non-traditional" experts, such as "biohackers". A biohacker is here defined as an individual who has technical experience in either innovating,

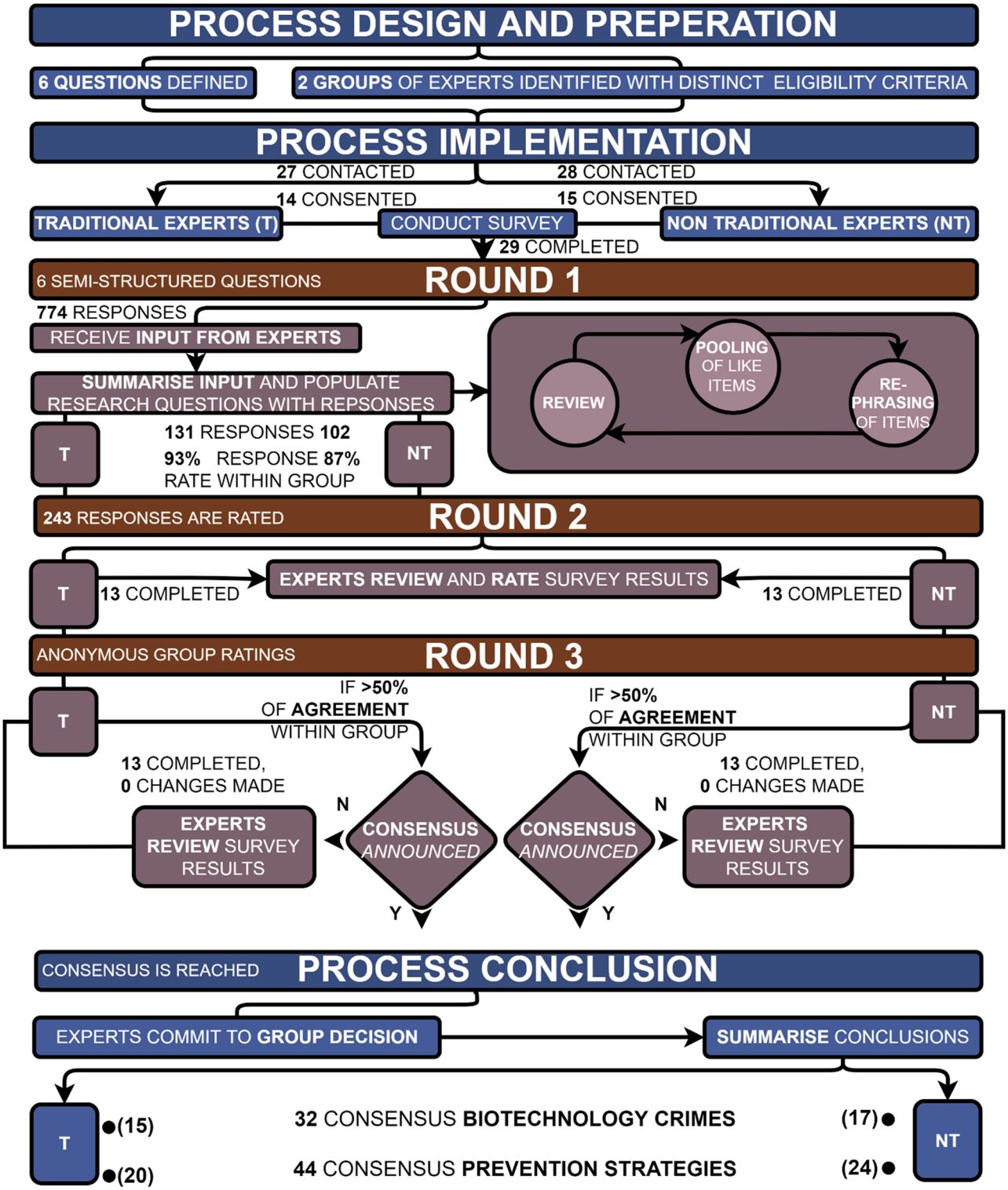


**Fig. 1.** Study design overview. See Section 2.5 for details.

developing or using biotechnologies, with or without professional or academic qualification, and who practices synthetic biology outside the institutional premise. Participants of this group were recruited based on previous fieldwork (see Methods section). It is important to note that we do not imply that either type of participant is associated with or participates in any of the activities and scenarios that emerged in the study. We believe that having two groups and using the opinions of recognised and "non-traditional"

experts is, however, important as the two groups may have very different views as to how the technology might develop or be exploited, and hence the crime opportunities that might emerge (including those that have not yet taken place).

The identification of these activities does, of course, depend on the definition of "crime". Crime is a social construct and local jurisdiction reflects the integration of ethics, culture and societal perspectives which can differ from border to border, highlighting the challenge of universal laws that could provide global protection. As this is continually informed by public opinion and adoption, what may be "illegal" today, may be legal tomorrow, and vice versa (for examples, see Evans, 1906). Given these complexities, we therefore use the term "crime" in this research interchangeably with the term "misuse" to include both currently illegitimate activities that are punishable by law (Bonger, 2015), but also emerging issues in biotechnology activities. Moreover, this broader scope of the term "crime" extends the otherwise dominant discussion in the biosecurity literature about weaponised misuse, which focuses primarily on biowarfare and bioterrorism (Vogel, 2008). Other aspects of bio-crime are relatively neglected, but important, and hence it is necessary to increase attention to this.

Taken together, this study focuses on eliciting and interpreting the opinions of experts regarding the threats posed by the biotechnology industry, including synthetic biology. The primary aim was to capture insight from experts and compare the responses from the two groups for the following key questions:

(i) what area(s) of biotechnology may be put to intended misuse, and
(ii) what is it that we should be doing now to prevent this activity.

In the following section we describe the methodological approach taken, including participant selection, the questionnaire used, and the survey approach.

## 2. Materials and methods

### 2.1. Ethics

Ethical approval was granted by the University College London Research Ethics Committee (REC) [reference number 15981/001] on 30th July 2019.

### 2.2. Study design

A parallel Delphi study was conducted with two groups of participants (traditional and non-traditional experts) across three survey rounds (see Fig. 1).

### 2.3. Recruitment and selection

A stakeholder mapping exercise was used to identify traditional experts within academia, industry and government. Stakeholders within the UK Government were identified using published organisation charts and were individuals who have had a responsibility for tracking developments in biotechnology and mitigating potential national risk. Academic stakeholders were identified through the list of authors identified in Elgabry et al.'s (2020a) systematic review, supplemented by further ad-hoc searches using google scholar. A list of industry stakeholders was identified from SynBiTech 2019, an international synthetic biology conference. The selection criteria for the traditional experts revolved around their level of training and experience in security, biotechnology and/or forecasting, Table 1.

**Table 1**
Participant description, eligibility and recruitment methods.

| | Traditional experts | Non-traditional experts |
|---|---|---|
| Eligibility criteria | • A level of training, biotechnology-related or security-related experience (1 or more years expertise),<br>• knowledge of public perception at a national level,<br>• have had previous engagement in forecasting or futures as part of their profession.<br>• Age range: 20 – 70 years old | • Their recognition within the community,<br>• 1 or more years expertise or experience in their profession<br>• newspaper records that discuss their activity,<br>• their activity<br>• Age range: 20 – 70 years old |
| Identification | Stakeholder mapping (including government, industry and academia) | Previous fieldwork |
| Recruitment | Email or in person | Email, social media or in person |
| Initially contacted | 27 | 28 |
| Round 1(number of participants) | 14 | 15 |
| Round 2 and 3(number of participants) | 13 | 13 |
| Retention rate | 93% | 87% |

Participants of this group included professionals in national security and intelligence, computational biology and cyber-biosecurity (Data in brief, Table 1). Out of the initial 27 traditional experts contacted, 13 did not respond.

Non-traditional experts were those with technical skills but who were involved in unconventional professions such as biohackers, ethical hackers and entrepreneurs in biotechnology-related start-ups. Biohackers are individuals who perform scientific experimentation outside the institutional premise, who may or may not have traditional (academic) qualifications (Yetisen, 2018). Ethical hackers are individuals who are authorised to penetrate systems, such as medical devices, and reveal potential security vulnerabilities. Non-traditional experts were identified through previous fieldwork conducted by the first author who attended the main biohacking conference, BDYHAX, in Austin, Texas in the United States in February 2019 and the main hacking conference, DEFCON, in Las Vegas, United States in August 2019. Non-traditional experts attending these conferences were recruited according to their technical skills and experience, including the "hacking" of biotechnologies and their recognition within the biohacking community. This was established through media records, social media presence and discussions with the community during fieldwork (Elgabry and Camilleri, 2021). Hacking is here defined as the act of recreationally, creatively or intellectually overcoming limitations of systems to achieve novel and clever outcomes (Sumida & Torisawa, 2008). Out of the initial 28 contacted, 13 did not respond.

Delphi studies often have high attrition rates (De Loë et al., 2016; Turoff, 1970) and so additional recruitment was conducted using a snowballing method (referrals from participants) (Denscombe, 1997) and chain referral (multiple snowballs) (Kalton, 1993) methods. As this study had a very specific focus and required the participation of highly specialised experts with interdisciplinary knowledge (biotechnology, security, biohackers), we aimed for a total sample size of 20 participants based on Akins et al. (2005) and Ogbeifun et al. (2016). Those who agreed to participate were asked to complete an expert profile questionnaire, which included a question about what they defined biotechnology to be, to establish their eligibility and to check that participants shared a common understanding of what biotechnology is (Data in brief, Table 1). All participants met our criteria and had a common view of what biotechnology is and hence were included.

A total of 29 (14 traditional and 15 non-traditional experts) geographically and culturally diverse stakeholders, from 7 countries, were interviewed in the first round. Participants were recruited from the UK (8/29), US (11/29), Canada (2/29), EU (Germany (1/29), Netherlands (4/29) France (1/29)) and Australia (2/29). Participants were recruited by email, in-person or through social media such as Twitter, Facebook and LinkedIn. Participants were provided with an information sheet (see Data in brief, Section 1.2) explaining the study and were asked to consent to participate, knowing that their participation would be anonymous, and that they could end their participation at any point. Participants within and across groups were anonymous to each other.

### 2.4. Questionnaire

The survey consisted of six "open" questions (see below), intended to elicit as much information as possible and to identify "scenarios".

1. In your opinion, do you think that there are area(s) of biotechnology that might be put to intended misuse in the next 5 years? Please elaborate.
2. What form(s) do you believe this activity (intended misuse) will take?
3. Who do you believe this activity (intended misuse) will affect the most? Why?
4. What steps should be taken now to address this potential future activity (intended misuse)?
5. Where (sectors, groups or geographies) do you believe this activity (intended misuse) is expected to first take place? Why?
6. Is anyone ultimately responsible for mitigating this activity (intended misuse)? Why? Who might that be?

Participants were also asked if there were any issues that they were not asked about that they thought we should be thinking about now. They were also asked if there was anyone else that they thought we should speak to who may be interested in participating in the study.

### 2.5. Procedure

In Round 1, participants were individually asked a set of six open questions (see above), either through an interview (in-person or virtual) or a digital survey questionnaire (influenced by the COVID-19 pandemic). This enabled the participation of respondents irrespective of geography and their availability (Rowe & Wright, 1999). We did not implement a time constraint between the first and second rounds to cater for potential time sensitivity in participants' professions (e.g. national security). A discussion with each participant (a total of 29 experts) independently generated a total of 774 responses. Considering the risks of revealing the information on misuse scenarios, we did not share details of the scenarios but instead provide summaries into themes. The input received from experts was summarised by pooling like responses to identify themes through grouping coded text (Thomas & Harden, 2008) and re-phrasing them to shorten and to populate the responses the experts needed to rate in the second round of the study. The traditional experts generated 131 responses, while the non-traditional group generated 102 responses. Of the 14 traditional experts that completed Round 1, 13 completed round 2 producing a 93% response rate within the group. Of the 15 non-traditional experts that completed Round1, 13 completed Round 2 producing a 87% response rate within the group.

Round 2 consisted of the same six questions, with populated responses from Round 1. Participants were individually presented with the themes identified in round 1 (for their group) and asked to rate the extent to which they agreed with them on a 7-point Likert scale (one indicating strong Agreement, and seven strong disagreement). In addition to rating each answer, comments were encouraged after each question.

In round 3, for each group, a summary of the group's overall ratings was sent to participants via email (Data in brief, Fig. 13-28). Having seen the group's ratings, all participants were given the chance to revise their ratings and were invited to specify their reasons. Nobody elected to change their initial responses, but a few participants justified their ratings where these differed from the group.

## 3. Results

The presentation of findings is divided into two sections: identified biotechnology misuses (Section 3.1) and proposed prevention strategies (Section 3.2). The former summarises the findings relating to the first four questions of the questionnaire (see Section 2.4), and the latter the responses to the last two questions. There is clear value in the identification of threats for which most agree it will not occur, as well as those for which most participants agree it will. That said, the identification of those threats for which there is the most agreement is valuable in helping to prioritise where effort should be invested, or concern focused first. As such, the results are organised with a focus on the eight areas (as sub-headings) for which there was agreement within the two groups first.

Perhaps ironically for a method intended to identify group consensus, there exists no strict agreement for what represents consensus in a Delphi study (Keeney et al., 2006). Here, we draw attention to those responses for which there was more than 50% agreement within a group. We start with the discussion of those scenarios for which the sum of the number of "Agree" and "Strongly Agree" scores of the group with an identified issue was more than 50%, and compare these responses across the two groups. We also comment on general observations regarding the full set of responses. We provide the rest of the information – where consensus was not reached – in Data in brief, Fig. 1-12. In addition to summarising findings, we provide example quotes from the traditional (T) and non-traditional (NT) groups to illustrate key points.

The first Delphi round initially yielded 774 ideas across the two groups (see Fig. 1) many of which overlapped. Through a thematic analysis (Thomas & Harden, 2008), these were distilled into a total of 233 topics (Data in brief, Table 2) – 131 for the traditional and 102 for the non-traditional groups. For 76 of the scenarios, of which 32 concerned biotechnology misuse and 44 concerned prevention strategies, there was 50% agreement within the group that identified them. Section 3.1 discusses these 32 misuse scenarios while Section 3.2 discusses the 44 proposed prevention strategies. In general, the responses differed between the two groups, but as discussed below (and in Section 4.3) eight scenarios overlapped.

### 3.1. Identified areas of misuse

Of the 32 scenarios, 15 were generated by the traditional group and 17 by the non-traditional group. When comparing the full responses for both groups, which can be found in the Data in brief section, there were more scenarios for which the traditional group (see Data in brief, Figs. 1–3) tended to agree, than there were for the non-traditional group experts (see Data in brief, Fig. 7-9).

Fig. 2 shows brief descriptors for each scenario (and a scenario number), ranked in descending order (for each group), for which there was high consensus in the traditional (T) and non-traditional (NT) expert groups. Four overlapping themes between the two groups, which we will discuss below by question (see questionnaire in Section 2.4), were: corporate espionage and cyber-biosecurity threats as identified intended misuses, that corporations will be affected the most by the identified intended misuses and that crime hotspots will include academia and China.

#### 3.1.1. Question 1

In terms of the technologies identified that might be put to intended misuse, only the traditional group reached consensus about what these might be, Fig. 2, Question 1. These were biotechnologies or data already found in the market such as CRISPR/Cas 9 gene editing (Fig. 2, #2), biological data (driven by commerce) (Fig. 2, #1), medical databases (Fig. 2, #5) and DNA synthesis technology (Fig. 2, #6) – which is consistent with the findings of Elgabry et al. (2020a). Although the NT group produced double the scenarios than the traditional group (Data in Brief, Supplementary Fig. 1 (T) and 7 (NT)), none had more than 50% agreement within the NT group (Data in Brief, Supplementary Fig. 7).

#### 3.1.2. Question 2

With respect to the types of misuse to which the technology might be put, two overlapping themes between the two groups emerged. These were corporate espionage and cyber-biosecurity threats. We will now discuss these, including any differing themes.

*3.1.2.1. Corporate espionage.* The traditional experts predicted that intended misuses would take various forms that were effectively either synthetic biology- or cyber-enabled crimes. Examples of the former were commercial/industrial espionage (Fig. 2, #15) such as stealing genetically modified seeds, or Intellectual Property (IP) theft (Fig. 2, #11) by biohackers who reverse engineer patented treatments (e.g. gene therapy). Non-traditional experts agreed that commercial fraud (Fig. 2, #118), particularly the selling of "snake oil" synthetic biology products is already occurring and that it is likely to increase. In line with the traditional group (Fig. 2, #15), non-traditional experts also agreed that corporate espionage is highly likely (Fig. 2, #120). Unlike the traditional group, they commented

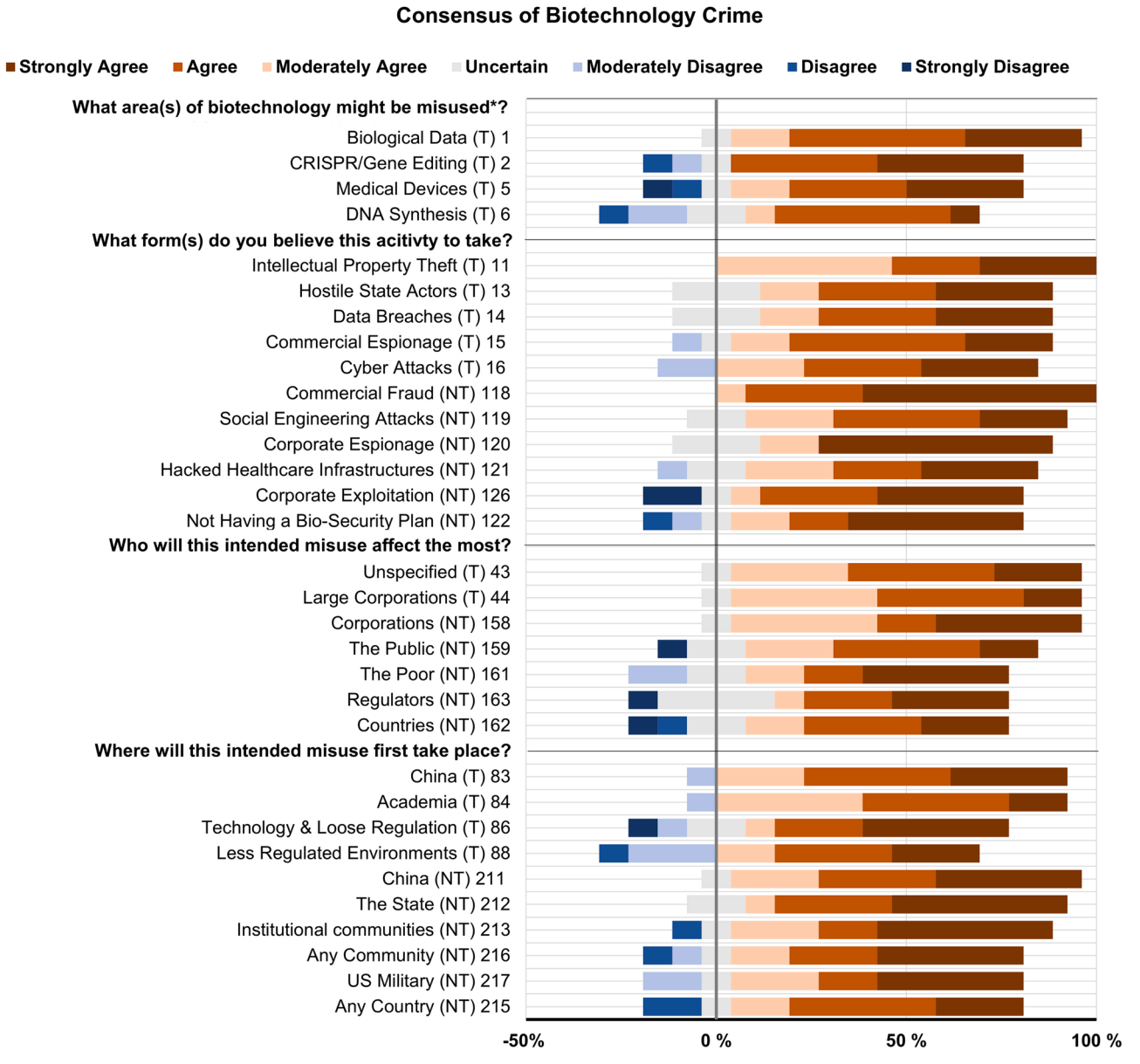


**Fig. 2.** Consensus for Biotechnology crime forms that the traditional (T) and non-traditional (NT) groups strongly agree are important in the next 5 years (Scenarios have been shortened in this figure. To see the full text of the scenarios, see Data in brief, Table 2).

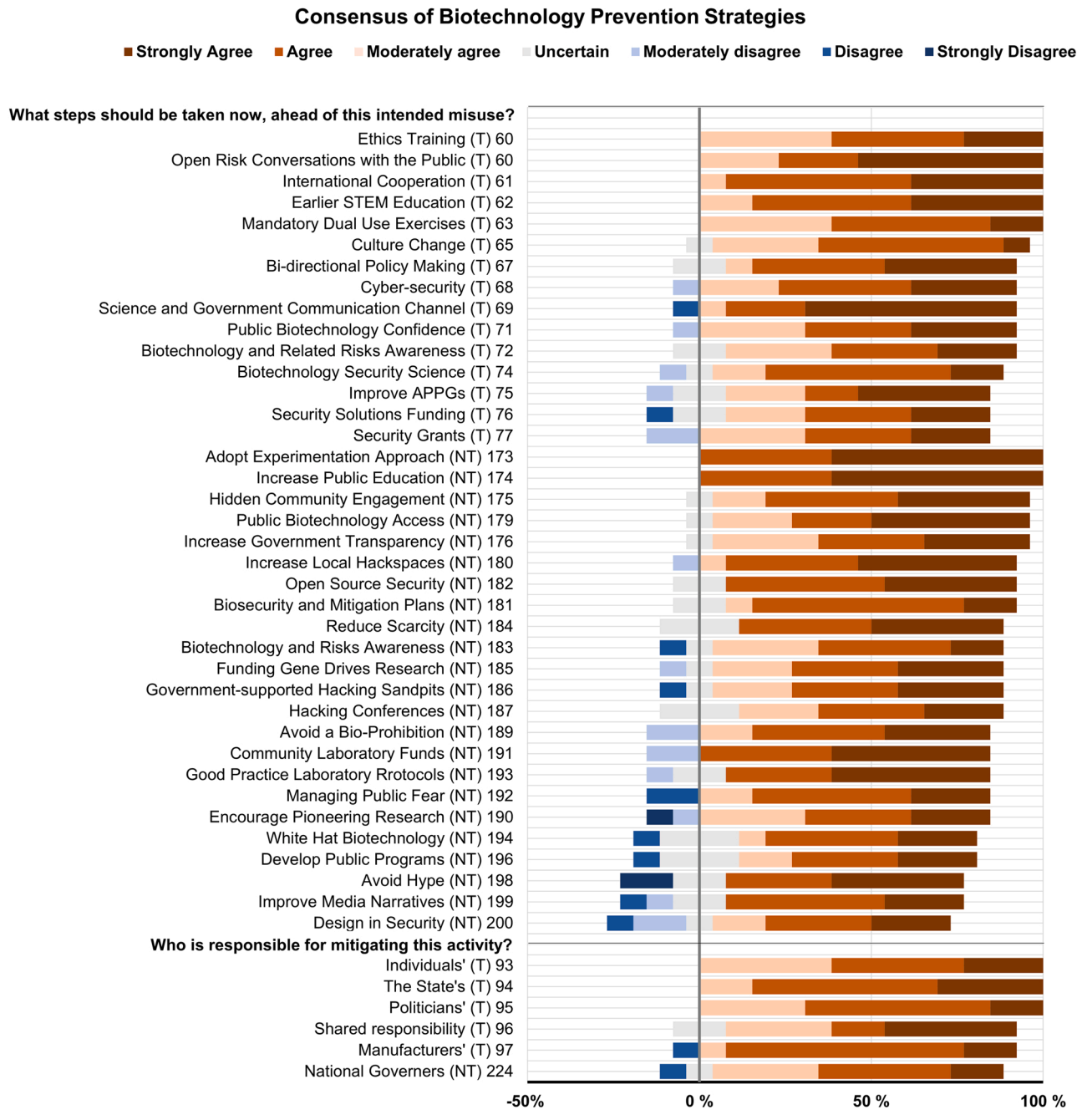


**Fig. 3.** Consensus for Biotechnology Prevention strategies that the traditional and non-traditional groups strongly agree are important. Scenarios have been shortened in this figure. To see the full text of the scenarios, see Data in brief, Table 2. (T) Traditional, (NT) Non-Traditional expert group.

on the negative unintended consequences that the industrialisation (past, present and future) of biotechnologies has had on human health and the planet, (Fig. 2, #126). Two examples of biotechnology companies were mentioned in particular, *Monsanto*[1] and *Weyerhaeuser*[2]. According to the non-traditional experts, these have contributed to climate collapse – as NT7 put it "*I would say that how we do agriculture is probably the most negative outcome of biotech usage,* while NT1 argued that "*70% of the pollution on the planet is done by 10 corporations*". Another concern mentioned was antibiotic misuse (Kardas et al., 2005) or overuse which is contributing to the

[1] An American agrochemical company acquired by Bayer known for using dangerous pesticides, for producing genetically modified organisms (GMOs), having a bad environmental record, and for having disputes with local farmers.

[2] An American timberland company that allegedly overcuts trees.

development of antibiotic resistance and has serious effects on health. One participant noted "*the antibiotic crisis – also a misuse in that sense, and climate change, which no one really has any solutions [for] and which is impacting everyone, everywhere, all the time - is unfolding slowly and is a much more complex problem to deal with*" (NT13). Whilst these were not discussed as malicious uses of biotechnology, the outcomes are nevertheless undesirable, potentially catastrophic and important to consider more generally.

*3.1.2.2. Cyber-biosecurity threats.* Examples of cyber-enabled crimes from the traditional experts were cyber-biosecurity threats to biotechnology workflows, databases and equipment, as well as threats to biological data. These, they predicted, would take the forms of cyber-attacks (Fig. 2, #16) on biotechnology infrastructures, devices, tools and techniques, medical device data breaches (Fig. 2, #14), or Hostile state actors misusing available biotechnology (Fig. 2, #13). One participant noted that "*Healthcare is a particularly compelling area for misuse. As the critical infrastructure sector is routinely cited as a soft target, which is a righteous way of saying that healthcare has focused on healthcare not security. Your health and body are tangible to folks and therefore scary. How much would a hospital pay to un-ransom their systems under normal conditions, but how much would they pay during a crisis such as COVID-19 or an act of terrorism*?"(T11).

The non-traditional experts also predicted that intended misuses of biotechnology would take cyber-bio-crime forms but, unlike the traditional experts, emphasised the vulnerability of the human factor in hacking (Fig. 2, #119). Social engineering (Mitnick & Simon, 2003) is the process by which sensitive information is elicited from people by exploiting vulnerabilities in processes intended to secure systems. For example, the theft of passwords (e.g. through phishing attacks) required to use biotechnology/cyber infrastructure, electronic health records and/or hospitals (Fig. 2, #121) can enable data breaches, identity theft and privacy concerns. With respect to bio-security plans, non-traditional experts agreed that it is the responsibility of those engaged in biotechnology to have such plans, but also that "*not having a plan or laughing at the concept*" (NT7) was poor biosecurity and was actually a form of biotechnology crime itself (Fig. 2, #122).

### *3.1.3. Question 3*

*3.1.3.1. Corporations affected by identified intended misuses.* The traditional experts agreed that offenders may not necessarily have specific targets (Fig. 2, #43), but that large bio-manufacturing, bio-pharmaceutical and well-known companies will be targeted due to their impact on the economy and the public (Fig. 2, #44). In contrast, Non-traditional experts agreed within their group that the security of medical devices would vary considerably and that the poor and the disenfranchised will be affected by this the most (Fig. 2, #161, 159). Three scenarios were raised in particular. The first was captured by a quote from one of the participants "*Make a medicine, charge the desperate"* (NT1). The second was the fact that devices with better security would be more expensive and hence beyond the reach of those with less resources. "*what Medtronics*[3] *has done is that they took that information [a reported insulin pump exploit] that was created during the hack, and they include parts of it [a security patch] in their future pumps but they also increased the price of those pumps astronomically. So the rich people continue to get to use those wonderful benefits of this modified pump that is actually more secure. However, the poor people are stuck with the old pump and stuck with those security risks*" (NT3). The third concern raised was an increasingly large biotechnology-related knowledge gap. As NT3 commented "*they [the poor] also have a knowledge gap that exists there too, where they have to find somebody that is smart enough to do that [patch the security vulnerabilities], have to get lucky or know somebody or work through their environment to find the correct person that can help them [patch the security vulnerabilities]"*. The concerns then were that rather than security being a default, that it would be provided at a premium and that it would require effort and know how to ensure its continued application.

### *3.1.4. Question 4*

*3.1.4.1. Academia and China as crime hotspots.* Traditional experts agreed that they expect biotechnology misuse to first take place in areas where the right technology exists (and therefore a capability of misuse exists), where there is loose regulation (Fig. 2, #86) and individuals with bad intent. They expected intended misuse of biotechnology to occur in China (Fig. 2, #83), in less regulated environments (Fig. 2, #88), and to emerge in academia and research groups (Fig. 2, #84). Some participants observed that academics might be victims noting, for example, "*It's unlikely that somebody ingrained in the academic environment is going to take the time to learn information security best practices*" (T1). Whilst others commented that misuse might occur in academic environments due to the fact that public understanding of the technology and legislation has not yet caught up with developments in academic research, as was seen with the application of CRISPR/Cas 9 technology on human embryos in 2018 (Regalado, 2018). As one participant commented "*There's academia and CRISPR babies in China, is it a crime, probably not. It caused an enormous outrage, and I think the majority of people would say this is a crime, even if not legislated for"* (T2).

Non-traditional experts also agreed that nations that do not welcome emerging technologies will be at risk (Fig. 2, #162). As an example, the technology of CRISPR/Cas 9 and the geographical dispute of the Western / Eastern debate was highlighted. Non-traditional experts agreed that regulators (Fig. 2, #163) will struggle to keep up with democratised biotechnology as it becomes more widely distributed. According to the non-traditional experts and similar to traditional experts (Fig. 2, #44), they agreed that this will also effect large corporations (Fig. 2, #158), as NT7 put it, "*in general the crime will be the infringement of IP of large corporations that*

[3] An American medical device company

*have spent years historically developing high value products*".

Like traditional experts, non-traditional experts agreed that biotechnology is not constrained to borders and will be exploited by criminals regardless of country (Fig. 2, #215). Moreover, that it could happen across a range of communities (Fig. 2, #216) to include academia and biohacking communities/hackspaces. However, they also agreed that the intended misuse is most likely to first occur in China[4] (Fig. 2, #211). Non-traditional experts reached a consensus of opinion that events of intended biotechnology misuse would first be expected to take place in sectors with funds, such as the US military (Fig. 2, #217) or Institutional communities (Fig. 2, #213). According to the non-traditional experts, individuals within these sectors conduct research and experimentation on a full-time basis (in comparison to Do-It-Yourself (DIY)/Biohacking communities), which may therefore lead to more opportunity for, or accelerate the possibilities for misuse. Non-traditional experts discussed the potential risk that might emerge from bottom up / grass root / DIY/ biohacking groups, but came to the consensus that this was not a key threat. Instead, they emphasised the threats associated with top-down actors such as the State (Fig. 2, #212). For example, a common view held and articulated by NT6 was that they were "*Far more concerned about the north Korean program than any individual DIY biologist – full stop*" (NT5).

### 3.2. Proposed prevention strategies

44 prevention scenarios were generated. 20 of these were suggested by the traditional group, 24 by the non-traditional group. When comparing the full responses of both groups (see Data in brief, Figs. 4-6 (T) and 10-12 (NT)), there tended to be more consensus regarding misuse prevention strategies than there had been for misuses of the technology. That said, there were more scenarios for which the traditional group (Data in brief, Figs. 4-6) tended to agree, than there were for the non-traditional group experts (Data in brief, Figs. 10-12).

Fig. 3 shows the prevention strategies, ranked in descending order (for each group), for which there was high consensus in the traditional (T) and non-traditional (NT) expert groups. Four overlapping themes between the two groups, which we will discuss below by question (see questionnaire in Section 2.4), were the need for: a radical change in culture, increased resources towards cyber-biosecurity governance, mitigation responsibility for national and international governors and avoiding a bio-prohibition through public literacy.

#### 3.2.1. Question 5

*3.2.1.1. A radical culture change needed.* Traditional experts highlighted a demand for a culture change (Fig. 3, #65) in the engagement of communities such as biohackers to create relevant legislation. As an example, according to traditional experts, biohackers would be the most appropriate individuals to develop their own ethics, policies and guidance for their community, as they most appropriately recognise their underlying problems and risks. In academia, traditional experts agreed that having lead scientists actively thinking of security implications (Fig. 3, #63) is imperative for preparedness against the potential misuse of developing technology and research. Traditional experts agreed that there is a need to introduce a security industry (Fig. 3, #74) similar to that in computing but applied to the Life Sciences, specifically to synthetic biology. For instance, according to the traditional experts, there is an unmet need to apply well-defined principles of cyber-security (Fig. 3, #68) into the life sciences such that equivalent firewalls, and intrusion detection systems are implemented, specific to synthetic biology/biotechnology.

Non-traditional experts agreed on the need for a more experimental approach (Fig. 3, #173) to better understanding the limitations of technology and that there is a need for freedom to innovate as a preventative step against biotechnology misuse. Suggested actions that non-traditional experts agreed on included supporting an open-source culture, increasing community laboratories (Fig. 3, #180) and welcoming "white hat" events (Fig. 3, #194) as a prevention strategy against potential reckless actors. "White hat" or ethical hacking is a security system penetration method that, according to non-traditional experts can be used as a countermeasure in combatting biotechnology misuse (Fig. 3, #187). Current successful models highlighted by the non-traditional experts include DEF-CON (a hacking conference in the US), where, according to the non-traditional experts, related communities (biohacker groups / grass roots individuals) can support the State against biosecurity threats – "*Hands down people at DEFCON and communities of the like are the reason why the US is still standing. And so I see DIY bio groups as grass roots ground swelling people with [the] ability to stop a lot of the biosecurity attacks*" (NT5). Consequently, and in realising this, non-traditional experts agreed that there is a need for the government to introduce a dynamic "area of play" (Fig. 3, #186) as a sandbox to test/push the boundaries of biotechnology. A "meta-process" could be put in place, according to the non-traditional experts, to update the sandbox area as new discoveries are made or accidents occur. As one participant noted, " [a] *sandbox in which people can play in such a way that we have the ability to expand this sandbox with new innovation. That really is one of the limits to many governmental structures because whenever you define the sandbox, someone immediately goes outside that sandbox and you're in a grey area. So there needs to be a meta-process to update our systems as we discover new things or as we cause accidents*" (NT5). To strengthen security, non-traditional experts agreed that Open-source security (Fig. 3, #182) could be implemented due to the faster turnaround in patching security issues.

*3.2.1.2. Increased resources towards cyber-biosecurity governance.* Traditional experts agreed that actions required to implement the suggested preventative steps include an increase in security-related funding (Fig. 3, #76) within biotechnology/synthetic-biology to

[4] A note to highlight that there was no representation from China in the participants of this study.

proactively engage in the security implications of emerging technology, "*If there's money for it, companies will compete for it to build a more secure solution*" (T3). According to traditional experts, these actions need to be coupled with improved communication channels between scientists (Fig. 3, #69), the public and the government. There was agreement between traditional experts that incentivizing research groups and companies through, for example, grant funds (Fig. 3, #77), will develop innovation and competition to build more secure solutions. Additionally, traditional group experts agreed that there needs to be a bi-directionality in policy making (Fig.3, #67) where the public debate should inform policy making and where implemented policy should inform the public. For this, traditional experts agreed that there is room for improvement in the role of All-party-parliamentary-groups (APPG)[5] (Fig. 3, #75) that, according to traditional experts, are currently failing.

### 3.2.2. Question 6

*3.2.2.1. National and international governors.* Traditional experts agreed that the mitigation responsibility is shared among individuals (Fig. 3, #93), manufacturers (Fig. 3, #97), politicians (Fig. 3, #95) and the State (Fig. 3, #94), with one participant noting that "*government has a responsibility but also establishments have to have responsibility on the things that they teach. There is also a risk of foreign investment and foreign students – [a] sovereign capability. Whether universities are keeping control on research that they are doing or whether that goes back to another country, whether we lose that skill or expertise, whether we're thinking about that – whether that then develops as a threat to the UK, someone develops something lethal and then goes back with the knowledge to develop that [elsewhere] and use it against you*" (T12).

In contrast, non-traditional experts strongly agreed with only one option regarding who is responsible (Fig. 3, #224): "*We need more trustworthy national governors and regulators; the more transparent they are, the more it allows for people around the world to comment and point out flaws*" (NT8). There were more suggestions on preventative measures from the non-traditional group than the traditional expert group (Fig. 3), which will now be discussed.

*3.2.2.2. Avoiding a bio-prohibition through public literacy.* Preventative steps, as agreed by traditional experts, would involve international cooperation (Fig. 3, #61), strengthening education in ethics (Fig. 3, #60), and biotechnology literacy (Fig.3, #72). Traditional experts agreed that increasing public genetic literacy and biotechnology awareness earlier through education and the promotion of STEM[6] subjects was necessary (Fig. 3, #62), with one participant noting, "*Do you mean kindergarteners? Because that's what I mean when I say the public! I think we should be teaching this stuff at the lowest possible levels and then all the way up, like electoral officials even at the very local level are being briefed on research that is going on in institutions that is going on inside their electoral zones – think that's super important.* "(T14). At the same time, traditional experts agreed that further training in ethics is required (Fig. 3, #60); especially when aiming to increase public confidence in biotechnology (Fig. 3, #71). "*Within the education of scientists, there could be more to educate them in this [ethics] area. I had some ethics courses in my own education but I don't think that they were necessarily taken very seriously by everyone because the examples were very general and not focused on the subjects we had an interest in. I heard from some people that they didn't get anything on this [ethics] at all during their entire education. There should be some sort of standard program or standard aspect in science education or biology to address this*" (T9).Non-traditional experts (Fig. 3, #174) agreed with the traditional experts (Fig. 3, #72) that it is necessary to increase public literacy about genetics and biotechnology awareness through education and mentioned a project pursued by a US-based biohacker that was described as an exemplar program by NT4, "*Make kids' engagement in science an everyday thing – like what is in NY - have a program to use [a] nanodevice for kids to DNA sequence one of the millions of plants that we don't have [a] sequence for and then they would publish a paper. And they would be published scientists. The kids would love it. Its [a] hook that would anchor them to science. It's a brilliant idea. We need more of that!"*.

Non-traditional experts highlighted the challenge of managing public opinion and fear (Fig. 3, #192) and agreed that messages from the media need to be improved. According to the non-traditional experts, the media must be engaged with (Fig. 3, #199) to stop the "hype" generated (i.e., distorting people's understanding of how much we know about biology and by doing so creating a culture of fear) (Fig. 3, #198). Non-traditional experts agreed that there is a need to alter how institutions and the government interact with communities, suggesting the benefits of partnerships (Fig. 3, #175). For example, one participant noted that there is a "*need to alter how institutions and especially the government interact with communities, [to] come at it as a partner and understand a true value for the betterment of the community and that's hard, that's a lot of mental shifting, looking at the processes that go on. That is the reduction of the corruption of the institutions, [that's] not an easy task"* (NT4). Non-traditional experts agreed on the following possible proactive actions: more exposure of the public to scientific/technical developments (Fig. 3, #179), laboratory protocols for good practice in community laboratories (Fig. 3, #193), hackspaces and biohacking garage laboratories. Non-traditional experts agreed with traditional experts that proactive security – rather than reactive - is needed by building security from the beginning rather than fitting it retrospectively (Fig. 3, #200). According to non-traditional experts, poor biosecurity results from a lack of awareness that biotechnology can be misused and, at the level of organisations, poor biosecurity occurs when infrastructure is not secure and there is no capability to respond to an incident quickly enough (e.g., using internal experts or when those are lacking, having the means for communicating to external experts) (Fig. 3, #181). Non-traditional experts agreed that increasing funding for community laboratories (Fig. 3, #191) and increasing local

[5] Informal cross-party groups (e.g., individuals and organisations) run by and for Members of the Commons and Lords that have no official status within Parliament.

[6] Science, Technology Engineering and Maths, and any subjects that fall under these four disciplines.

hackspaces (Fig. 3, #180) could increase capacity for prevention. For example, they discussed the possibility of "experimental" work performed at a small scale to better understand the boundaries of technologies (e.g., gene drives and their effect on ecological systems) including how they might be misused with the aim of developing countermeasures. As an example of a countermeasure to genetically modified organisms, "kill switches"[7] (Chan et al., 2016) were described by the non-traditional experts with one participant stating, "*we need to embrace the inevitability of a biologically fluid society and ecosystem and encourage regulators to do the same. I would like to avoid a bio prohibition, which I think is ultimately futile, and instead focus on countermeasures, kill switches, etc*." (NT15). An example of "experimental work" performed that was mentioned by the non-traditional experts, was the controversial use of the emerging CRISPR/Cas 9 by He Jiankui; the first (publicly announced) genetically engineered babies. While acknowledging the ethical issues implicated in editing human embryos, non-traditional experts highlighted that there could be negative implications of banning such applications of CRISPR/Cas 9 editing through a "*bio-prohibition*" (Fig. 3, #189).

## 4. Discussion

Trends in crime and security associated with biotechnology remain difficult to predict. Yet, advances in biotechnology, as with other technology continue at a rate faster than that of its security. Moreover, the discussion of security implications is limited to siloed expertise from traditional professions and there has been no engagement with diverse communities. This parallel Delphi study elicited opinions and forecasts that provide meaningful insights to help anticipate what these emerging trends might be and what might be done about them and by who. The methodological choice of including a non-traditional expert group was considered important to capture a wider threat (and solution) landscape, and this choice was supported by the additional and diverse scenarios generated. In this section, we first summarise our findings, beginning with the divergence of opinions between the non-traditional and traditional groups. We then summarise the divergence of opinions within the non-traditional group since they had more polarised views than did the traditional group. Finally, we present the eight scenarios that the traditional and non-traditional experts agreed on, which form the basis of a proposed set of multi-sector interventions to address them.

### 4.1. Divergence of opinions between the non-traditional and traditional group

We make note of the differences between the two expert groups as "divergence" of opinions, and highlight that this may not necessarily mean disagreement between them. Seven differences were found between the two expert groups on the predicted misuse of biotechnology, and four were observed for prevention strategies. Briefly, traditional experts predicted areas of biotechnology misuse to include DNA synthesis (Fig. 2, #6) and gene editing (Fig. 2, #2), while non-traditional experts considered unintended consequences (Fig. 2, #126) and not having a biosecurity plan as a misuse itself (Fig. 2, #122; Fig. 3, #181, 193). The non-traditional experts also indicated that the poor and disenfranchised will be affected the most from the intended misuse of biotechnology (Fig. 3, #184). Additionally, the non-traditional experts agreed that regulators and countries that do not embrace emerging technology (Fig. 2, #162) will be affected the most, while traditional experts agreed within their group that it would depend on the motives of perpetrators (Fig. 2, #43). Finally, another difference between the two groups related to their approach to proposed prevention strategies. The need for international cooperation was highlighted by the traditional group, in contrast to the non-traditional group that stressed the need for an open source / open security community and platform (Fig. 3, #173, 182, 186, 187, 189, 194, 200). The following sub-sections expand on some of these points of divergence.

### 4.2. Insights from traditional group on DNA editing technologies

The Traditional Group identified gene editing tools as a future facilitator of biotechnology misuse (Fig. 2, #2). As DNA synthesis costs continue to drop, gene editing capabilities extend beyond the boundaries of specialised laboratories and highly skilled personnel, into highly accessible tools such as DIY kits and CRISPR / Cas 9. Their potential widespread use in the future may increase risks of misuse. This is in agreement with the results of Elgabry et al.'s (2020b) systematic review that, despite the low number of extracted articles, revealed evidence on crimes that could be facilitated by synthetic biology. This suggests that the current opinion of members of industry and government coincides with that of the academic literature. Albeit the profound benefits of the peer review process for quality research, the rate at which academic literature is published could introduce a delay in the recency of information the government and industry receive, which suggests the need for other forms of information sourcing regarding emerging trends.

### 4.3. Insights from the non-traditional group on a biosecurity plan

Non-traditional experts agreed that there is a responsibility for those engaged in biotechnology to have biosecurity plans (Fig. 3, #181, 193) that include both intended misuses but also unintended consequences (Fig. 3, #184). Indeed "responsible innovation" or the collective stewardship of science, has been and, arguably, continues to be a major challenge in contemporary democratic governance (Stilgoe et al., 2013; Macnaghten et al., 2014). Stilgoe et al. (2013) developed a framework to address innovation inherent socio-ethical concerns using four dimensions: anticipation, reflexivity, inclusion and responsiveness. Anticipation aims to increase

[7] Otherwise referred to as "biocontainment systems," "kill switches" in biological organisms are genetically engineered to prevent growth (kill) of target cells when an external substance is present (Chan et al., 2016)

resilience by asking "what if" questions that may reveal risks in the research and any opportunities in avoiding these. Reflexivity refers to being aware that there is no universally held framing of issues and that there should be inclusion of voices in governance and policymaking from a wider public; which may be uneven. Finally, responsiveness or the ability to change the direction of the research given these inputs (e.g., public values) is necessary to go beyond compliance and towards responsible innovation. This is similar to the "sandbox" concept proposed by the non-traditional experts who participated in this study (Section 3.2.1, NT5).

### 4.4. Insights from the non-traditional group on media communication

Non-traditional experts agreed within their group that there is a need to change the media narrative around biotechnology, its applications and potential misuses (Fig. 3, #198, 199). "Avoiding hype" was raised by the non-traditional group only. This may be attributable to negative media coverage that biohackers have received in the past (e.g., Bromwich, 2018; Smalley, 2018). Being aware of the effects/influences of media communication on public perception and understanding, may also explain some hesitancy of some self-identifying as biohackers (and being connected to bad press that may suggest wrong doing/practice of science) found in the literature and previous fieldwork conducted by the first author (Trejo et al., 2020; Elgabry and Camilleri, 2021). This may need to be carefully considered when engaging with the biohacking community to improve communication channels between scientists (Fig. 3, #69), the public and government, as suggested by the traditional group, too.

### 4.5. Divergence of opinions within the non-traditional group

When comparing the two groups' distribution of responses, the non-traditional experts generated more scenarios than the traditional group and were more likely to "strongly agree" or "strongly disagree" with the scenarios generated. While there could be many reasons for the polarity observed within the non-traditional group, one may be because the non-traditional group comprised individuals with varied expert profiles (Data in brief, Table 1). As an example, see Data in brief, Figs. 15 and 16 that present the low consensus in forms of biotechnology misuse of each group.

### 4.6. Convergence of opinions between the non-traditional and traditional group

We consider the overlapping scenarios between the two expert groups to represent a "convergence" of opinions. There were eight overlapping scenarios; six related to the misuse of biotechnology and four to prevention strategies. Briefly, both groups predicted that biotechnology misuse will take the form of device and/or data breaches (Fig. 2, #1, 5, 14, 16; #121), and corporate exploitation (Fig. 2, #11, 15; #118, 120, 126). Both groups agreed that corporations (Fig. 2, #44; #158) and/or State actors (Fig. 2, #13; #212) will be affected the most from biotechnology misuse and that this is expected to first take place where there is technological capability, such as in academia (Fig. 2, #84; #213) or in countries such as China (Fig. 2, #83; #211). It is important to highlight here that none of the participants of the study were from China and that both traditional and non-traditional groups comprised of participants predominantly from the US and Europe, (see Section 2.3). Given the limits to the geographic diversity of the participants, while the way in which China has been identified as a source of threat may appropriately reflect the views of the participants, other countries might have been considered to represent high risks for biotechnology crime, had there, for example, been more participants beyond the US and Europe. Both groups of experts also agreed that education (Fig. 3, #59, 60, 62, 63, 72; #174, 176, 180, 180, 196), providing funding (Fig. 3, #76, 77; #191) and governance (Fig. 3, #94; #224) would be important components of prevention strategies against biotechnology misuse. The following sub-sections expand on some of these common points that form the basis of our proposed multi-sector interventions.

#### 4.6.1. Establishment of a biotechnology security and crime science

As suggested by both expert groups in this study (Fig. 3, #59, 60, 62-3, 72; #174, 176, 180, 183, 196), we encourage the establishment of training or curriculum in a Biotechnology Security and Crime Science (Fig. 3, #74). In line with the resulting recommendations of NASEM, in building and sustaining a skilled workforce (National Academies Press, 2020), this would focus on aiding professionals in the Life Science with security acumen and relevant security actors with an understanding of the life sciences, so that future threats can be better anticipated and solutions designed. Founders of the cyber biosecurity field have already commenced efforts towards this agenda by suggesting synthetic biology modules that can be introduced to security professionals (Adames et al., 2019). However, the language and definitions used between the professionals of each discipline still require clarification, as discussed below.

As biotechnology becomes increasingly connected, cyber risks extend to the Life science domain (Mueller, 2021). To understand and address the threats that may emerge will require conceptual and legal clarity about what is considered a cybercrime and what is considered a biocrime. As defined by Jansen et al. (2014), a biocrime refers to the use of a biological agent to cause harm to an individual / group of individuals through extortion for ransom or revenge. Definitions of cybercrime vary (Gordon & Ford, 2006), from crime committed by means of computers or the internet (Moore, 2005), to the more detailed UK Government's National Cyber Security Strategy's definition that distinguishes between a traditional crime that can be committed using information technology (Cyber-enabled) or crimes that can only be committed through the use of information technology (Cyber-dependent)[8]. Elgabry et al. (2020a)

[8] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

applied this concept to biotechnology and proposed a similar division for Biotechnology -dependent or enabled crime. Such a distinction may help the right professional identify threats earlier and should be given consideration.

Crimes at the intersection of the cyber / life science domains and their classification will have to be considered carefully, as they may currently be under-reported as their forms may be unknown or undetectable. Both traditional and non-traditional experts agreed that biotechnology is not constrained to borders and will be exploited by criminals regardless of country. In common with this, the inherent (and ongoing) challenge of unlocalised threats within cyberspace persist, both in terms of identifying the origin of the attack and the attacker's non-geographic cyber-identity (Papadimitriou, 2009). As is illustrated by the controversies regarding the origins of the SARS-CoV-2 virus (Rasmussen, 2021; Segreto & Deigin, 2021; Malaiyan et al., 2021; Casadevall et al., 2021), similar issues may increasingly emerge for biological threats and consideration should be given to how to deal with such issues.

#### 4.6.2. *Changes in governance to engage with non-traditional communities*

Both expert groups agreed that changes to current governance arrangements are necessary. The traditional group proposed bi-directionality in policy making (Fig. 3, #67), improving All-party-parliamentary-groups that according to the traditional experts are currently failing (Fig. 3, #75) and engaging with diverse communities for relevant legislation (Fig. 3, #65). Similarly, the non-traditional group agreed that it is necessary to change how institutions and the government interact with communities (Fig. 3, #175).

The biohackers interviewed as part of the non-traditional group were recruited through previous fieldwork conducted by the first author (Elgabry and Camilleri, 2021). However, the biohackers recruited in this study were predominately from the United States. This was largely because the visibility of the biohacking community in the UK is low. Strengthening communication (see Section 4.3) with the biohacking community can act as a harm reduction tactic. Considering the benefits of engaging with this community, the non-traditional group generated more scenarios than did the traditional group of experts (see Data in brief, Figs. 15-18). This could be useful in forecasting exercises such as horizon scanning and/or scenario building as more possibilities would be generated during the assessment of potential risks. While some of these may be wildcards that are unlikely to happen, the most successful approach to prevention is likely to be the one (or ones) that can address the most (likely) scenarios. Consequently, identifying the widest possible set of scenarios, however probable, is important for policy formulation.

Considering approaches taken in different countries, there is currently no clear communication channel, reporting system or engagement pathway within the biohacker community in (say) the United Kingdom. This contrasts with the model adopted in the United States (US), where the FBI engages directly with biohackers through community laboratories and by sponsoring synthetic biology conferences (Wolinsky, 2016). The inclusion of non-traditional experts in the iterative process of identifying, classifying, prioritising, remediating, and mitigating vulnerabilities through enhanced vulnerability management may contribute to (biotechnology) crime prevention efforts (Elgabry, 2020; Evans et al., 2020) and is worth pursuing in countries outside of the US.

The government's role in encouraging or enforcing this integration will be important. There is impalpable benefit of innovation and social change catalysed by the biohacking community, but it must be done so carefully to ensure safety. To benefit from these activities, we therefore suggest governments increase engagement with the biohacking community at hackspaces, with careful consideration in clearly defining the experimental landscape.

#### 4.6.3. *Development of an experimental framework for continuous inquiry*

The (diversity of) views expressed by the expert groups in this study alone, and in fact from any other forecasting exercise, will only inform future biosecurity and public health policy for a limited time horizon because things are changing at such pace. That is, there is a need for a complimentary experimental framework that will allow for a continuous inquiry on emerging misuses, that is coupled with practical suggestions.

For this, we propose the combination of the Delphi process with the hackathon model (Halvari et al., 2019) as a proof-of-concept framework. "Hackathon" refers to a design sprint-like event bringing domain experts to collaborate intensively on a project. This hybrid approach can be used as a red-teaming approach to aid national security decision-making for risks on emerging technology (see Elgabry, 2021) and has been recognised in the UK's National Security Machinery First Report[9].

### 4.7. *Limitations and future work*

The input received from diverse stakeholders and the process for soliciting and incorporating their feedback are the strengths of our study. As a future piece of work, the segmentation of the opinions and forecasts by nation would be beneficial as each region may have a different perceived tolerance of risk. As an example, it is expected that the responses from individuals from the United States would differ from those of (say) the United Kingdom if asked how they stay safe in everyday life (i.e. protection through ownership of arms).

Additionally, forecasting crime trends using this Delphi process but with a younger participatory group may increase the generation of scenarios that may otherwise be limited by professional roles. For example, this could be delivered to students through an exercise that starts by engaging them in an interactive lecture regarding ethics in biotechnology and subsequently invites them to participate in a workshop. In the workshop, half the class could be asked to identify possible future crimes that could exploit a biotechnology, while the other half could be asked generate ideas to prevent misuses of it. We suggest this should be extended as future work in pursuit of a standard approach to responsible innovation (Stilgoe et al., 2013) in biotechnology and related studies.

[9] https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/157608/senior-parliamentarians-criticise-failures-in-government-security-planning/

Finally, we are currently piloting the Hackathon Delphi model on ingestible emerging technology (see Elgabry, 2021). Outcomes of the Delphi process will inform participants' prototyping of their devices as well as security by design principles through a policy briefing, and we advocate that this approach be used more widely.

## 5. Conclusion

We used data-driven input from key biotechnology and security stakeholders of both traditional and non-traditional expertise that generated opinions and forecasts for emerging crime trends facilitated by biotechnology to devise a multi-sector crime prevention strategy plan in preparation for future biotechnology crime.

We proposed interventions across sectors of industry, academia, government and policy to help prepare international governments to make informed decisions about their involvement in future biotechnology developments, including a framework for engaging with the biohacking community. By investing in security and building a cyber-biosecurity infrastructure, innovation can be driven forward whilst reducing the likelihood of an unintended crime harvest.

## Author contributions

M.E. conceived and carried out the study and data analysis. M.E. wrote the initial manuscript, S.D.J. and D.N. contributed to revising this manuscript. All authors read and approved the final manuscript.

## Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Data availability

We have shared my data at the Attach File step.

## Acknowledgments

The authors would like to acknowledge the EPSRC and the DAWES Centre for Future Crimes at UCL that funded and supported the research.

## Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.futures.2022.102970.

## References

Accademia Nazionale dei Lincei. (2020). COVID-19 vaccines: Fall report.
Adames, N. R., Gallegos, J. E., Hunt, S. Y., So, W. K., & Peccoud, J. (2019). Hands-on introduction to synthetic biology for security professionals. *Trends in Biotechnology, 37*(11), 1143–1146.
Agapakis, C. M. (2014). Designing synthetic biology. *ACS Synthetic Biology, 3*(3), 121–128.
Akins, R., Tolson, H., & Cole, B. (2005). Stability of response characteristics of a Delphi panel: Application of bootstrap data expansion. *BMC Medical Research Methodology, 5*(37), 37. https://doi.org/10.1186/1471-2288-5-37
Bonger, W.A. (2015). An introduction to criminology. Routledge.
Bromwich, J. E. (2018). Death of a biohacker. The New York Times, May, 19.
Brown, K. V. (2020). One biohacker's improbable bid to make a DIY Covid-19 vaccine. Bloomberg; ⟨https://www.bloomberg.com/news/articles/2020-06-25/one-biohacker-s-imbrobable-bid-to-make-a-diycovid-19-vaccine⟩. Butler, Review of Intelligence.
Casadevall, A., Weiss, S. R., & Imperiale, M. J. (2021). Can science help resolve the controversy on the origins of the SARS-CoV-2 pandemic?.
Chan, C. T., Lee, J. W., Cameron, D. E., Bashor, C. J., & Collins, J. J. (2016). "Deadman" and "Passcode" microbial kill switches for bacterial containment. *Nature Chemical Biology, 12*(2), 82–86.
Coutorie, L. E. (1995). The future of high-technology crime: A parallel Delphi study. *Journal of Criminal Justice, 23*(1), 13–27.
Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458–467.
Dalkey, N. C., Rourke, D. L., Lewis, R., & Snyder, D. (1972). *Studies in the quality of life; delphi and decision-making*. Lexington, MA: Lexington Books.
Denscombe, M. (1997). *The good research guide*. Buckingham: Open University Press.
Elgabry, M., Nesbeth, D., & Johnson, S. D. (2020a). A Systematic Review of the Criminogenic Potential of Synthetic Biology and Routes to Future Crime Prevention. *Frontiers in bioengineering and biotechnology, 8*, 1119.
Elgabry, M., Nesbeth, D., & Johnson, S. D. (2020b). A systematic review protocol for crime trends facilitated by synthetic biology. *Systematic reviews, 9*(1), 1–8.
Elgabry, M. (2020) "National Biosecurity: Cyber-Biosecurity Written Evidence" UK Parliament Joint Committee on National Security and Biosecurity, UK Parliament.
Elgabry, M. (2021) "National Machinery: Red-Teaming Approach Written Evidence." UK Parliament Joint Committee on National Security and Machinery, UK Parliament.
Elgabry, M. and Camilleri, J. (2021) Conducting hidden populations research: A reflective case study on researching the biohacking community, Futures.
Erickson, J. (2008). *Hacking: the art of exploitation*. No Starch Press.

Evans, S. W., Beal, J., Berger, K., Bleijs, D. A., Cagnetti, A., Ceroni, F., & van Passel, M. W. (2020). Embrace experimentation in biosecurity governance. *Science, 368* (6487), 138–140.
Evans, E. P. (1906). The criminal prosecution and capital punishment of animals. London William Heinemann. ⟨https://www.gutenberg.org/files/43286/43286-h/43286-h.htm⟩.
Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology, 2*(1), 13–20.
Halvari, S., Suominen, A., Jussila, J., Jonsson, V., & Bäckman, J. (2019). Conceptualization of hackathon for innovation management. The International Society for Professional Innovation Management (ISPIM). ⟨https://search.proquest.com/conference-papers451proceedings/conceptualization-hackathon-innovation452management/docview/2297094456/se-2?accountid=14511⟩.
Heidt, A. (2020). Self-experimentation in the time of COVID-19. The Scientist; ⟨https://www.thescientist.com/news-opinion/self-experimentation-in-the-time-of-covid-19-67805⟩.
Jansen, H. J., Breeveld, F. J., Stijnis, C., & Grobusch, M. P. (2014). Biological warfare, bioterrorism, and biocrime. *Clinical Microbiology and Infection, 20*(6), 488–496. https://doi.org/10.1111/1469-0691.12699. PMID: 24890710; PMCID: PMC7129974.
June, C. H., O'Connor, R. S., Kawalekar, O. U., Ghassemi, S., & Milone, M. C. (2018). CAR T cell immunotherapy for human cancer. *Science, 359*, 1361–1365. https://doi.org/10.1126/science.aar6711
Kalton, G. (1993). Sampling considerations in research on HIV risk. In D. G. Ostrow, & R. C. Kessler (Eds.), *Methodological issues in AIDS behavioral research* (pp. 53–72). New York: Plenum Press.
Kardas, P., Devine, S., Golembesky, A., & Roberts, C. (2005). A systematic review and meta-analysis of misuse of antibiotic therapies in the community. *International Journal of Antimicrobial Agents, 26*(2), 106–113.
Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: Ten lessons from using the Delphi technique in nursing research. *Journal of Advanced Nursing, 53* (2), 205–212.
Kirkpatrick, J., Koblentz, G. D., Palmer, M. J., Perello, E., Relman, D. A., & Denton, S. W. (2018). *Editing biosecurity: Needs and strategies for governing genome editing.* George Mason University.
Lentzos, F., Goodman, M. S., & Wilson, J. M. (2020). Health security intelligence: Engaging across disciplines and sectors.
Linstone, H. A., & Turoff, M. (Eds.). (1975). *The delphi method* (pp. 3–12). Reading, MA: Addison-Wesley.
De Loë, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the state of policy Delphi practice: A systematic review evaluating methodological evolution, innovation, and opportunities. *Technological Forecasting and Social Change, 104*, 78–88.
Macnaghten, P., Owen, R., Stilgoe, J., Wynne, B., Azevedo, A., de Campos, A., … Garvey, B. (2014). Responsible innovation across borders: Tensions, paradoxes and possibilities. *Journal of Responsible Innovation, 1*(2), 191–199.
Malaiyan, J., Arumugam, S., Mohan, K., & Gomathi Radhakrishnan, G. (2021). An update on the origin of SARS-CoV-2: Despite closest identity, bat (RaTG13) and pangolin derived coronaviruses varied in the critical binding site and O-linked glycan residues. *Journal of Medical Virology, 93*(1), 499–505.
Mitnick, K.D., & Simon, W.L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
Moore, R. (2005). *Cybercrime: Investigating high-technology computer crime*. LexisNexis.
Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosafety and Health, 3*(1), 11–21.
Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Frontiers in bioengineering and biotechnology, 39*.
National Academies Press. (2020). *Committee on safeguarding the bioeconomy: Finding strategies for understanding, evaluating, and protecting the bioeconomy while sustaining innovation and growth*. Washington, DC: Safeguarding the Bioeconomy. ⟨https://www.nap.edu/download/25525⟩.
National Academies of Sciences, Engineering, and Medicine (NASEM) (2017). An evidence framework for genetic testing.
The National Academies of Sciences Engineering Medicine (2015). Meeting Recap, Safeguarding the Bioeconomy: Applications and Implications of Emerging Science. Organized by Board on Chemical Sciences and Technology (Washington, DC). Available online at: https://www.ehidc.org/sites/default/files/resources/files/Safeguarding%20the%20Bioeconomy_II_Recap%20Final%20090815.pdf.
The National Academies of Sciences Engineering and Medicine (NASEM) (2014). Meeting Recap, Workshop – Convergence: Safeguarding Technology in the Bioeconomy. Organized by the Board on Chemical Sciences and Technology and the Board on Life Sciences (Washington, DC).
National Academies of Sciences, Engineering, and Medicine. (2018). Biodefense in the age of synthetic biology.
Nieuwenweg, A. C., Trump, B. D., Klasa, K., Bleijs, D. A., & Oye, K. A. (2021). Emerging biotechnology and information hazards. *Emerging threats of synthetic biology and biotechnology* (pp. 131–140). Dordrecht: Springer.
Ogbeifun, E., Agwa-Ejon, J., Mbohwa, C., & Pretorius, J. (2016). *The Delphi technique: A credible research methodology*. Kuala Lumpur: International Conference on Industrial Engineering and Operations Management.
Papadimitriou, F. (2009). A nexus of Cyber-Geography and Cyber-Psychology: Topos/"Notopia" and identity in hacking. *Computers in Human Behavior, 25*(6), 1331–1334.
Pease, K. (1997). Predicting the future: The roles of routine activity and rational choice theory. In G. Newman, R. V. Clarke, & S. G. Shoham (Eds.), *Rational choice and situational crime prevention: Theoretical foundations* (p. 233). Aldershot: Dartmouth.
Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From naive trust to risk awareness. *Trends in Biotechnology, 36*(1), 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012
Ran, F. A., Hsu, P. D., Wright, J., Agarwala, V., Scott, D. A., & Zhang, F. (2013). Genome engineering using the CRISPR-Cas9 system. *Nature Protocols, 8*, 2281–2308. https://doi.org/10.1038/nprot.2013.143
Rasmussen, A. L. (2021). On the origins of SARS-CoV-2. *Nature Medicine, 27*(1), 9-9.
Regalado, A. (2018). EXCLUSIVE: Chinese scientists are creating CRISPR babies. MIT Technology Review.
Rowe, G., & Wright, G. (1996). The impact of task characteristics on the performance of structured group forecasting techniques. *International Journal of Forecasting, 12*, 73–89.
Rowe, G., & Wright, G. (1996). The impact of task characteristics on the performance of structured group forecasting techniques. *International Journal of Forecasting, 12*, 73–89.
Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting, 15*(4), 353–375.
Segreto, R., & Deigin, Y. (2021). The genetic structure of SARS-CoV-2 does not rule out a laboratory origin: SARS-COV-2 chimeric structure and furin cleavage site might be the result of genetic manipulation. *BioEssays, 43*(3), Article 2000240.
Smalley, E. (2018). FDA warns public of dangers of DIY gene therapy. *Nature Biotechnology, 36*(2), 119–121.
Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(9), 1568–1580.
Sumida, A., & Torisawa, K. (2008). Hacking wikipedia for hyponymy relation acquisition. In *Proceedings of the third international joint conference on natural language processing: volume-II*.
Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research, 8*, 45. https://doi.org/10.1186/1471-2288-8-45
Trejo, M., Canfield, I., Robinson, J. O., & Guerrini, C. J. (2020). How biomedical citizen scientists define what they do: It's all in the name. *AJOB Empirical Bioethics, 12* (1), 63–70.
Turoff, M. (1970). The design of a policy Delphi. *Technological Forecasting and Social Change, 2*(2), 149–171.
Vogel, K. M. (2008). Framing biosecurity: An alternative to the biotech revolution model? *Science and Public Policy, 35*(1), 45–54.
Wolinsky, H. (2016). The FBI and biohackers: An unusual relationship. *EMBO Reports, 17*(6), 793–796. https://doi.org/10.15252/embr.201642483
Yetisen, A. K. (2018). Biohacking. *Trends in Biotechnology, 36*(8), 744–747.