BIOSECURITY

Assessing the bioweapons threat

Is there a foundation of agreement among experts about risk?

By **Crystal Boddie,[1] Matthew Watson,[1] Gary Ackerman,[2] Gigi Kwik Gronvall[1]***

The U.S. government (USG) has taken steps intended to diminish the likelihood of misuse of research—in one recent action, declaring a funding moratorium on gain-of-function studies on influenza until a risk-benefit analysis can be conducted (*1*). The analysis is expected to examine biosafety concerns, the potential for such research to produce a biological weapons agent, and the possibility that publication may lower barriers to bioweapons development (*1*). To analyze the security risks of biological research, however, it is first necessary to determine the likelihood that bioweapons will threaten national security and to what degree legitimate research is at risk of misuse. This type of assessment is fraught with uncertainty.

POLICY

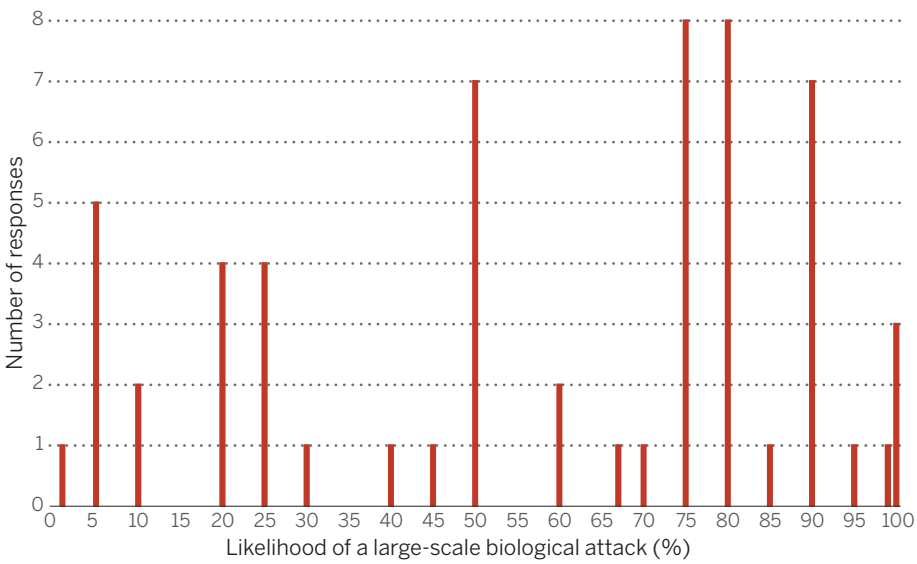
Empirical data for threat assessment is sparse: Thankfully, there have been only a handful of historical examples of bioterrorism or biowarfare (use by a nation state), although multiple nations and terrorist organizations have developed the capability to varying degrees. Intelligence about bioweapons programs and intent to use them has been difficult to acquire; miscalculations include type 1 errors (Iraq was thought to have a biological weapons program during the lead up to the Second Gulf War, at which time it did not) and type 2 errors (the former Soviet Union was not thought to have a biological weapons program but, in fact, employed tens of thousands of weapons scientists). Given the paucity of other data, judgments about the bioweapons threat rest largely on expert opinions. Understanding how experts in national security, biosecurity, and biosafety perceive the bioweapons threat is therefore important for assessing the threat, as well as the potential for misuse of legitimate research.

ASSESSING COLLECTIVE JUDGMENTS. We used a Delphi method study to elicit, combine, and analyze the collective judgments of multiple experts. Focused on obtaining collective expert opinion, but avoiding "groupthink," the Delphi method's salient features are preserving the anonymity of participant inputs, iterated response and feedback, and statistical aggregation of expert judgments (*2*). Individuals were invited to participate in this study if they held responsibility for shaping public policy at the nexus of life science and national security or on the basis of their expertise and knowledge in the field or the recommendations of other participants (using a snowball sampling methodology). Participant affiliations included USG and former USG; academia; and nongovernmental, private sector, and industry organizations. The participants had responsibility for shaping public policy from ~3 to more than 45 years. Participant training and background included biological and nonbiological science, medicine, public health, national security, political science, foreign policy and international affairs, economics, history, and law. Of the 63 experts originally approached to participate, 62 completed the first round of the survey, and 59 completed the second round.

Participants were asked to respond anonymously to questions about biological threats, review each other's answers, and either amend or maintain their answers after reflecting on others' opinions. They were asked to supply rationales for their responses (*3*). The process was terminated when the mean response did not change more than one standard deviation across all questions, which occurred after two rounds (*4*). Results were analyzed with STATA statistical package 11.2 and Wilcoxon-Mann-Whitney nonparametric tests (significance level $P \leq 0.05$).

LIKELIHOOD OF A BIOWEAPONS ATTACK. We asked participants to estimate the percentage likelihood of a large-scale biological weapons attack occurring within the next 10 years in any country (see the first chart). We defined a large-scale attack conservatively, as resulting in more than 100 ill people. There was a wide diversity of opinions. Participants' answers ranged from 1 to 100% likelihood, with a mean of 57.5%, [95% confidence interval (CI) 49.4 to 65.7]. In general, those trained as biological scientists perceived a lower likelihood of bioweapons use than other participants ($z = 2.9$, $P = 0.0035$), although that was certainly not true in every case. Also, participants classified as members of the Baby Boomers and/or Silent Generation (50 years of age or older) believed the likelihood of attack was greater than did Generation X and/or Millennials (21 to 49 years of age); with mean responses of 64.6% and 46.0%, respectively ($z = -2.1$, $P = 0.035$).

Likelihood of attack. What do you estimate to be the likelihood of a large-scale biological weapons attack occurring within the next 10 years?



THE MOST LIKELY ACTOR AND AGENT. Participants were also asked about the likelihood of different types of state and nonstate actors to be the perpetrator of a biological weapons attack within the next 10 years. Although participants held a wide range of

[1]UPMC Center for Health Security, University of Pittsburgh Medical Center, Baltimore, MD, USA. [2]Unconventional Weapons and Technology Division, National Consortium for the Study of Terrorism and Response to Terrorism (START), University of Maryland, College Park, MD, USA.
*Corresponding author. E-mail: ggronvall@upmc.edu

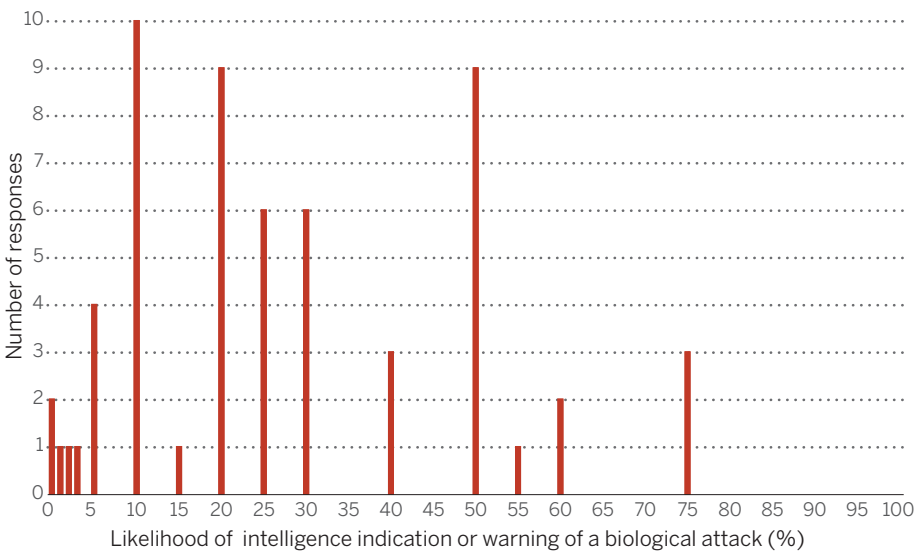
opinions, overt state bioweapons use was considered to be less likely than covert use by a state or use by a nonstate group. An overt attack by a state actor was rated significantly less likely than even the next lowest rated actor: criminal groups ($z = -3.9$, $P < 0.001$). Religious extremists were judged to be the most likely group to perpetrate an attack—significantly more likely than a covert attack by a state actor ($z = -3.6$, $P < 0.001$) or any other attack by a state but not significantly more likely than a right-wing violent nonstate actor or a disgruntled or mentally ill individual. Participants who were especially concerned about terrorist use cited rapid technological advances in the biosciences, ease of acquiring pathogens, democratization of bioscience knowledge, information about a nonstate actors' intent, and the demonstration of the chaos surrounding the Ebola epidemic in West Africa in 2014 as support for their views. Those more concerned about the nation-state threat cited the technological complexities of developing a bioweapon, the difficulty in obtaining pathogens, and ethical and/or cultural barriers to using biological weapons. Pathogen access and the technical complexity required to produce a biological weapon were cited as support for opposite conclusions about potential actors.

We also asked about types of biological agents likely to be used as weapons within the next 10 years. Participants felt that the likelihood of use was highest for biological toxins. This was followed by spore-forming bacteria, non–spore-forming bacteria, and viruses. Participants generally did not think that fungi and prions were likely to be weaponized and felt that the likelihood of a synthetic pathogen being used as a weapon in the next 10 years was fairly low (*4*).

Since 2001, a point of emphasis for the U.S. intelligence community (IC) has been the prevention of the use of a weapon of mass destruction. Despite IC efforts, however, most participants believed that intelligence agencies are unlikely to provide actionable information or warnings before a biological attack (see the second chart). Of 59 participants, 53 considered there to be a 50% or lower probability that a warning would be forthcoming in advance of an attack.

Although a few participants felt that the IC had improved their level of access and detection capabilities, many cited the difficulties inherent in detecting and tracking biological weapons capabilities owing to biology's dual-use nature; the ease of concealing preparations for a biological attack; limitations in expertise and investment in biological threats by the IC; and past experiences of the challenges associated with intelligence collection against biological threats. The realities of classification of information make a fully informed analysis of IC capabilities vis-à-vis the biological threat impossible—a fact that several participants acknowledged.

Likelihood of actionable warning. If a biological attack were being planned today, what is the probability that intelligence information will provide actionable indications and warning preceding the attack?



RED LINE FOR RESEARCH. Our study also obtained participants' judgments about acceptable limits for U.S. biodefense, particularly "threat characterization" laboratory studies (usually classified) that are performed to gain knowledge about potential bioweapons for purposes of defense (i.e., is there a "red line" that should not be crossed?). Most said yes (51), but there was a wide variety of opinions of what types of research would cross that line.

Three participants felt that the only "red line" for biodefense is human subjects research and that all other defensive research that furthers national security should be allowed. A majority of participants said that research that violates the Biological and Toxin Weapons Convention crosses a red line and should not be pursued. Two participants felt that threat-characterization research should not be conducted at all because of the inherent risks. Of the participants, 27 mentioned gain-of-function experiments as a situation where a red line could be drawn. Even under the secure conditions of threat-characterization research, there was a lack of consensus among experts about where the "red line" should be drawn and whether that line is gain-of-function research.

RISK OF MISUSE OF RESEARCH. The potential for devastating consequences if biological weapons were used is enough to spur planning. Yet, given the scantiness of the historical record, it is not surprising that experts reached different conclusions about the likelihood of a biological weapons attack. Highly classified intelligence, if available, may have reduced the degree of variation; given the importance of a shared, informed perception of the threat in order to prepare, investments should be made to acquire intelligence on biosecurity threats and share with relevant parties.

The diversity of views, even in this experienced group of participants, means that it will be more challenging to assess the risks that research would be misused and to develop a regulatory system for legitimate dual-use research. Risks and benefits should still be examined and recommendations made about the conduct of this or other research. However, a red line for what is allowable and what is forbidden in the name of security may not be clearly defined, and the way forward will be nuanced and complicated, possibly requiring a case-by-case evaluation with guidelines agreed upon by the scientific and policy communities. ■

REFERENCES AND NOTES

1. White House Office of Science and Technology (S&T) Policy, "Doing diligence to assess the risks and benefits of life sciences gain-of-function research" (White House, Washington, DC, 2014).
2. G. Rowe, G. Wright, *Int. J. Forecast.* **15**, 353–375 (1999).
3. G. Rowe, G. Wright, in *Principles of Forecasting*, J. S. Armstrong, Ed. (Springer, New York, 2001), pp. 125–144.
4. See the supplementary materials for further details.

ACKNOWLEDGMENTS

We thank the participants in the Delphi study, as well as the S&T Directorate, U.S. Department of Homeland Security, for funding and support.

SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/349/6250/792/suppl/DC1

10.1126/science.aab0713