Strategy for Biological Risk & Security

Drew Endy
MIT Biology & Biological Engineering
http://mit.edu/endy/

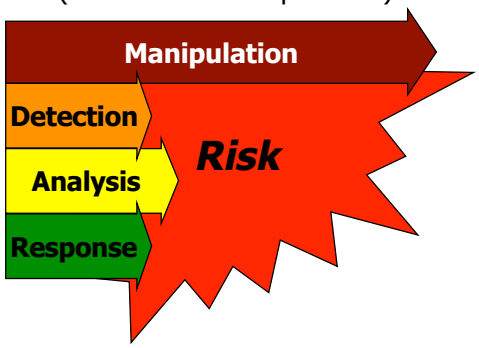
Document Background:

The material in this document is taken from the DARPA ISAT Synthetic Biology study that I chaired and which finished in October of 2003. Minor edits have been made to reconcile context. The ISAT study was neither classified or published. I am making this material available in the hopes of promoting the development and implementation of a strategy for directly addressing the issue of future biological risk.

Terms of Use:

Why do biological risks exist?

Technology Classes Relevant to Biological Risk
(current relative capabilities)



Endy, Drew [endy@mit.ed]

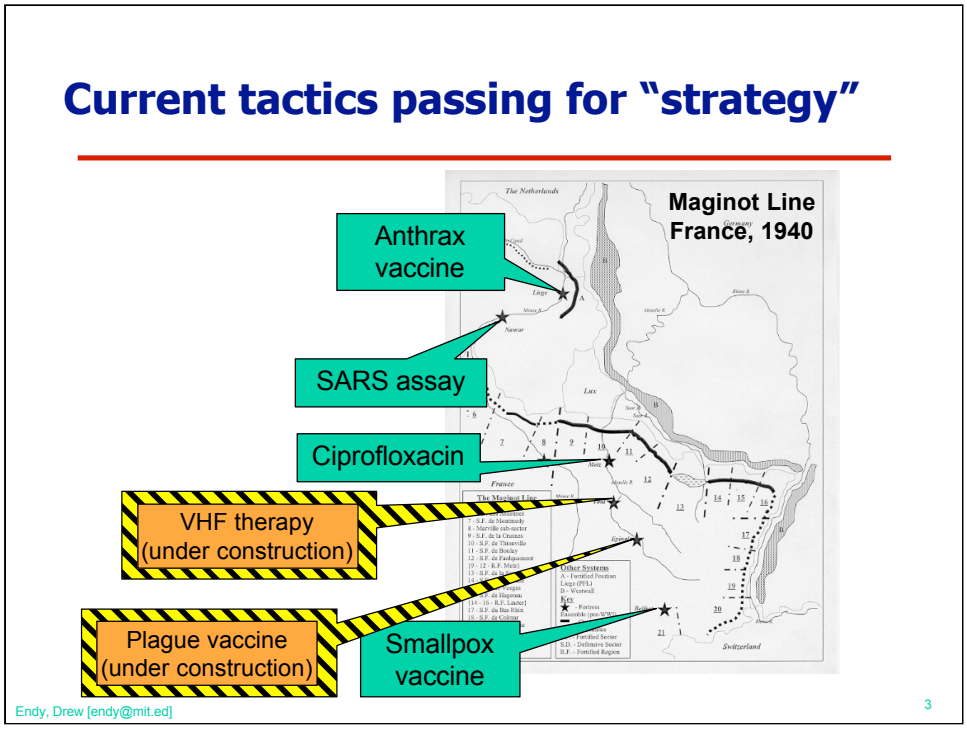
2

Both nature's, and our own, ability to manipulate biological systems outpaces our ability to detect biological agents, analyze the resulting data, and respond appropriately. As a result, we risk exposure to existing, emerging, and engineered biological threats (graphic above).

Two issues dominate discussions of biological risk. First, the "dual-use" dilemma as it relates to biological technology - any useful technology might also be intentionally or accidentally misapplied to cause harm. A recent National Academies report provides expert background, analysis, and discussion of the dual-use dilemma for past and current biotechnology - see Fink et al., National Research Council of the National Academies (2003), "Biotechnology Research in an Age of Terrorism: Confronting the "Dual Use" Dilemma." Second, the probable inability to control the distribution of technologies needed to manipulate biological systems and, lacking advances in other technology classes (i.e., detection, analysis, and response), a consequent increasing future vulnerability to engineered biological threats.

Can the current gap between manipulation and detection, analysis, and response be closed?

Do technologies that enable biological engineering help or hinder closure of the risk gap?



The "conventional wisdom" within the biological research community is that current threat dynamics are largely driven by nature, and take the form of emerging infectious diseases. For example, the 2002 SARS outbreak killed more people than the 2001 anthrax attacks; both would pale in comparison to a repeat of the 1918 influenza pandemic. Many biologists ask if it is possible to intentionally "improve" existing pathogens, somehow bettering nature's designs. Importantly, the rate of natural threat emergence is slow enough such that the development and deployment of threat-specific responses are oftentimes considered to be "adequate."

The experience of the biological research community with modern technology-based risk dates to the creation of recombinant DNA technology - in the 1970s it became possible to create chimeric DNA absent a perfect ability to predict the properties of the resulting molecule. Today, three additional factors are beginning to impact the biological risk landscape: (i) public databases of DNA sequence and computation-based design tools are enabling rapid and "lab-free" access to knowledge of what DNA to synthesize, (ii) public access to DNA synthesis is enabling anonymous fabrication (e.g., website, credit card, and FedEx), (iii) individuals might act to intentionally misapply biological engineering technologies.

In considering these new factors, it seems obvious that future biological threats will increasingly arise via the intentional or accidental (i.e., "michanikogenic") application of biological technology. Importantly, the rate of biological threat emergence is likely to become great enough to overwhelm current response technologies. We are (appropriately) developing and deploying "fixed assets" against existing, relatively-static biological threats(graphic above). However, future biological risks are likely to be greater in number, more sophisticated in design and scope, and more rapidly developed and deployed.

Thus, we need to transition to a capabilities-based strategy for dealing with future biological risk. The effectiveness of such a strategy could be characterized by three statistics:

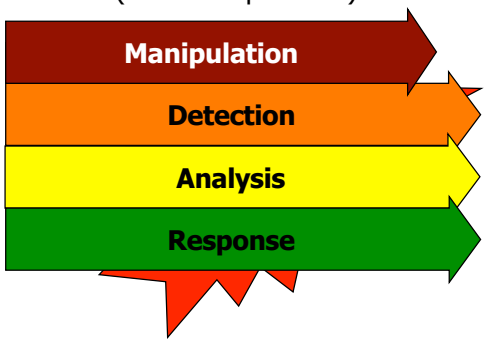
(1) How long does it take us (in days) to detect a new emerging infectious disease or engineered agent?

(2) How long does it take us (in days) to understand how the agent works such that we can respond as needed?

(3) How long does it take us (in days) to delivery a response?

A future strategy based on technology?

Technology Classes Relevant to Future Biological Risk
(needed capabilities)



Endy, Drew [endy@mit.ed]

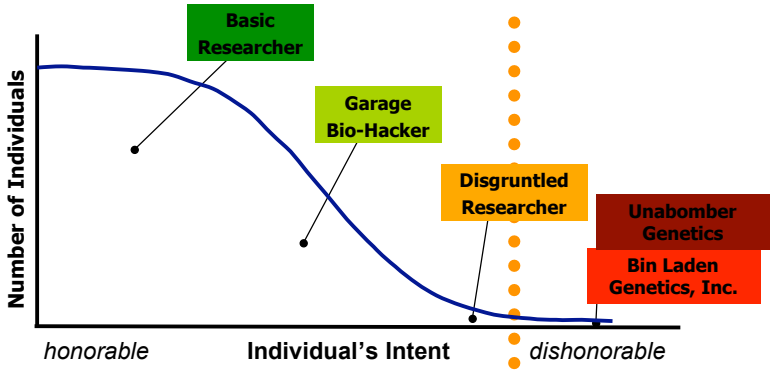
4

A conservative discussion of strategy for minimizing biological risk would begin with three grounding assumptions. First, that we already can not control the distribution of technology and information enabling the manipulation of biological systems and that future technologies are also unlikely to be controllable. Second, ineffective attempts to forbid access to some of the basic technologies for manipulating biology would likely incur prohibitive costs in the form of lost opportunities for improving human health and gaining scientific knowledge. Third, that threats could arise from nature, nation states, loosely organized groups, and individuals, and could be targeted against any part of the living world relevant to human welfare (i.e., biological threats are asymmetric in (i) source of agent, (ii) choice of target, and (iii) time to construct versus respond, below).

Given the above context, the rate of detection, analysis, and response to new threats becomes critical; a biological agent that took years to evolve and emerge, or be engineered and released, might require coordinated detection, analysis, and response within weeks. In addition, the breadth of possible targets requires that detection, analysis, and response capabilities be as general as practically possible and are, at least in part, accessible to a distributed network of end users. By analogy, computer network security relies heavily on the fact that all users have access to tools and resources for the detection, analysis, and response to network threats - but note that any net contribution via distributed security requires that most users have a vested interest in maintaining network function (next page).

Technologies enabling the engineering of biology would directly contribute to a rapid and predictable response to biological threats (e.g., pre-positioning components of standard vaccine vectors, 24h synthesis of DNA encoding multi-antigen-domain proteins, et cetera). In addition, a cadre of engineers familiar with the design of biological systems would help to enable more rapid threat analysis.

Suite of solutions



Endy, Drew [endy@mit.ed]

5

However, the same technologies that are needed to help enable rapid responses to new biological threats could also be used to help construct the threats themselves. Thus, a strategy for addressing future biological risk must consider how future techologies can be best combined with non-technical solutions in order to minimize both the number of sources of future biological risks, and the scope of the risks themselves. What steps can be taken now, at the beginning of the field, to minimize the number of individuals who could or would act to cause harm via future biological technology (graphic above)?

As one obvious example, biological engineering training could include professional development programs and codes of ethics; a well conceived and responsibly implemented plan for educating future generations of biological engineers would help to expand strategic human resources for future biological defense. As a second example, registries managing standard biological parts could encourage responsible practice on the part of commercial DNA synthesis providers (e.g., "we'll only renew our synthesis contract if you can assure us that you are not synthesizing known threat agents").

Non-technical approaches contributing to future biological security might range from legal incentives and penalties, to social rewards and stigmatization, to methods of training and practice, et cetera. Much more investigation and discussion of the role of non-technical components in a suite of solutions for biological risk mitigation is warranted.