Bulletin of the Atomic Scientists

# Is the availability of genetic information dangerous?

BY GIGI KWIK GRONVALL, IRIS HUNGER, JENS H. KUHN, AND LEONID F. RYABIKHIN | 8 NOVEMBER 2007

The genetic information of organisms--as varied as goldfish and geraniums--is widely available to the global public. So are the biologic codes for many viruses, such as variola (which causes smallpox) and poliovirus. The advance of biological technologies that allow for the construction of specific genetic sequences raises the harrowing possibility that someone, somewhere would use available genetic information to unleash a biological attack. The quandary facing scientists in the life sciences is similar to the issues that confronted scientists at the dawn of the nuclear age: Can potentially dangerous knowledge be made secret? Or should it be kept widely avaialbe? Below, our four discussants explore the dangers of keeping genetic information public.

## We're all responsible for biosecurity

IRIS HUNGER | 28 FEBRUARY 2008

Because we all agreed early on--for one reason or another--that most genetic information should remain freely accessible, this discussion turned quickly to the more general question of what information to oversee, limit, or even prevent and how to do it. This question has worried experts for a while. And though the answer is neither straightforward nor simple, it's a necessary question.

In response to the question about what information should be overseen, limited, or prevented, most scientists would say that higher risk information deserves more intrusive oversight. Scientists have compiled several lists of "risky" research. The often-quoted Fink report lists seven classes of experiments of concern, including experiments that increase transmissibility of an agent and enable the evasion of diagnostic and detection methods. The CISSM oversight proposal mentioned earlier categorizes activities into extreme, moderate, or potential concern; activities of extreme concern would include research with eradicated or BSL-4 agents. In 2002, Raymond Zilinskas and Jonathan Tucker proposed a list of six types of "sensitive" activities, including facilitating dissemination as a fine particle aerosol and improving stability of pathogens.

All of these lists are similar. Most mention synthesizing viruses as a problematic activity. And all seem to take into account which agents will work effectively as bioweapons. Despite these similarities, scientists and experts are not close to

agreeing about what constitutes risky activities. After all, the pathogen is only one part of a bioweapon. The dissemination mechanism is the second part, and it is often overlooked. Some of the participants in this roundtable, particularly Jens Kuhn, have referenced "weaponization," but we didn't properly discuss the subject. Discussions about risky weaponization activities address factors such as the open-air release of agents, methods for aerosol immunization, or the use of viruses as transport vehicles. Dissemination methods are important because, in most cases, they spell the difference between a bioweapon attack with limited effects and a mass casualty attack.

Most existing and proposed oversight procedures focus on research before it begins--for good reason. However, some research results are completely unexpected (see the legendary mousepox research in Australia) so projects need to be reviewed after they're done as well. So far, however, post-research oversight is left to individual scientists and is voluntary. Will this work? It's unlikely. A soon-to-be published survey by the Research Group for Biological Arms Control at the University of Hamburg shows that most major English-, Russian-, and Chinese-language life science journals have not implemented security review procedures, despite calls for them to do so.

All existing and proposed oversight approaches only work when they are implemented widely, ideally on a global scale. Whether pulmonary plague breaks out in Washington, Berlin, or Nairobi it will reach all corners of the globe sooner rather than later. Implementing good oversight in one country will have a limited effect. But how do scientists go about making oversight international? Many states place biosecurity very low on their national agendas; they have other problems to address, for example, hunger, AIDS, or corruption. Biosecurity oversight typically follows biotech industry development, though most sensitive research projects are still done in the Western world, even though biotechnologies are rapidly expanding across the globe. So, for the moment, Western states bear the biggest part of the responsibility to protect the public. They still can and should influence the conduct of biological research worldwide to prohibit the hostile use of biotechnology.

## Why biodefense research is necessary

LEONID F. RYABIKHIN | 20 FEBRUARY 2008

Bioscience and biotechnology have an inherent dual-use nature, and genetic information, as an integral part of bioscience, has the same nature. So, yes, the availability of genetic information is dangerous. Because the potential misuse of this information poses a threat, the information needs to be controlled or regulated. What these control mechanism should look like and how they are implemented are complex issues. But we cannot ignore this problem.

At the dawn of nuclear physics, all scientific information related to the field was open. But most of this information disappeared from open sources when Germany, Britain, the United States, and the Soviet Union launched nuclear weapons programs. Nowadays, anyone can find descriptions about how to make a nuclear bomb on the internet, but the essential portion of sensitive information is still

classified and restricted. From whom and why? From potential adversaries and "bad guys," such as terrorists, rouge states, and irresponsible regimes.

I agree with Gigi Kwik Gronvall that the lack of direct experience developing bioweapons could be overcome with trial and error. But the lack of such experience and information make this job very hard and maybe impossible. When control regimes work, they make this task even more difficult. Scientists should not exempt genetic or other biological information that can be unpredictably harmful to humans and nature from such controls.

What should be controlled? Two options for control exist: controlling access to information or controlling the use of information. A well-balanced combination of these two options would be preferable. I support a few of the interesting points made by my colleagues in this discussion. Iris Hunger and Jens Kuhn raise the possibility of the deliberate generation of dangerous genomes, and this is exactly the type of information whose access should be restricted.

I agree that bioscientists and security experts should work together to install an oversight system, such as that proposed by the Center for International and Security Studies at Maryland. Additionally, we need to ensure the free access of genetic information for developing biodefense countermeasures in coordination with responsible organizations and licensed specialists. The free access to scientific information is, after all, a main condition for scientific and technological progress. But scientists should work to find the proper balance between free access to information and control over its use.

Like many experts, I don't think that any state or terrorist organization will use bioweapons or bioagents in the near future. Matt Meselson gave many reasons for this in his January/February 2007 *Bulletin* interview. Among the strongest arguments are the lack of political and military rationales for their use. Yet, because a large-scale bioattack coincides with the terrorists goals, nations need to build robust and effective biodefense systems. They should base these systems on two key elements: early warning--surveillance, monitoring and even epidemiological intelligence--and a developed public health system capable of responding to dangerous disease outbreaks--both natural and artificial. The participants in this roundtable all understand the challenges we face and the necessity to probe broadly for solutions.

## The biosecurity risks not yet addressed

JENS H. KUHN | 15 FEBRUARY 2008

It is a relief to me as a bench scientist, but a positive surprise to me as a biodefense professional, that all of the discussants in this roundtable argued in favor of publicly available pathogen sequences. This is an indication of the closing gap in thinking between life scientists and policy experts. In the past, this gap has made it difficult for either group to understand and accept the viewpoints of the other. Pathogen sequences *need* to be available to every scientist, argue the scientists, because otherwise research would come to a screeching halt or at least be impeded

dramatically. Pathogen sequences *can* be available to every scientist, argue the policy experts, because the information is impossible to control or to withdraw, and transparency in research trumps secrecy. Both groups are largely in agreement on the availability of pathogen sequences being of no great help to terrorists. It is the *weaponization* of agents, rather than their acquisition through in vitro synthesis, that is most difficult for terrorists to achieve, although how difficult it really is will remain a focus of future debate.

This roundtable has not adequately addressed the risks that publicly available sequences may pose in the future once scientists create artificial organisms, resurrect extinct agents, or make more virulent or more transmissible known pathogens, either accidentally or deliberately. Iris Hunger correctly argues that we need transparency in these areas of research first and foremost and that the more dangerous a research agent (or project), the greater the concern should be. While I am absolutely in favor of the public deposition of any sequence derived from any finished research project, I also favor a priori oversight and consequently possible disapproval of planned research in areas where it is foreseeable that "dangerous" sequences may be created in the absence of a clear public benefit. The emphasis here lies on *foreseeable*.

I disagree with Gigi Kwik Gronvall's view that the CISSM oversight system would not be a net gain for biosecurity. She argued that it "would slow down science a great deal." However, I demonstrated in a working paper that the system would only affect a very small percentage of researchers and institutions. Only high- and maximum-containment facilities, which already are subject to other oversight requirements, and researchers that plan a very limited set of deemed-to-be-risky experiments (making an agent more transmissible or multi-drug resistant, etc.) would fall under the system.

The issue of what makes an agent dangerous, which set of experiments could be considered risky, and what should be overseen is, of course, contentious, as Gronvall points out. But this did not stop the Fink Committee of the U.S. National Academy of Sciences from outlining what it considered to be dual-use "experiments of concern." Moreover, researchers can and should be able to modify the list of covered research activities to keep pace with changes in science and technology, as has been done for over 30 years for recombinant DNA research. I also don't think that the CISSM system would necessarily require scientists "to devote many hours to the review process [of planned experiments]," as the system is tiered and requires oversight on either the local (i.e. within an institution through, for instance, the already existing institutional biosafety committees), national, or international level depending on the planned project. Some oversight could also be integrated into the grant-review process, thereby further involving bench scientists in the review system.

Finally, that there might not be 100 percent participation in a dual-use review system is not a legitimate argument for dismissing it out of hand. I suggest that how all of this could or would not work be the focus of a follow-up roundtable discussion.

## The unintended consequences of biosecurity solutions

GIGI KWIK GRONVALL | 6 FEBRUARY 2008

As the roundtable winds down, I've begun to reflect on what I've learned from the conversation and what can be done to move the subject forward. We are in agreement that genetic sequences should remain available. Our supporting arguments for this position vary, as do our emphases on what's important, but surprisingly, we are in general agreement.

Our opinions differ, however, about the difficulty of making and using a biological weapon, and whether states or small groups are of greater concern. I think it would be far less difficult to make and deploy a biological weapon than some of the other participants on this roundtable believe. I believe most states can produce bioweapons if they want, but that small groups can as well, and I find that more worrisome. Time will tell if this is an accurate assessment. While each of our judgments are all likely to be wrong in some way, let us hope that we are all wildly wrong in every way and that biological researchers are able to safeguard their work for the benefits of health and knowledge.

Jens Kuhn proposed following the international oversight system set forth by the Center for International and Security Studies at Maryland (CISSM) to ensure that future. I agree with the intended purpose of the CISSM system, and it is an excellent starting point for discussion. But it has several flaws, and its implementation would not be a net gain for biosecurity. For example:

- the likely speed of the research review proposed by the plan could slow down science a great deal, driving scientists in dual-use disciplines to go to other areas of research, or to work around the system;
- the issue of "who decides?" what areas of research require oversight could be extremely contentious and may not reflect the real risks inherent in a proposed experiment;
- the oversight system is unlikely to encompass all international biology research, particularly as several countries see biotechnology as a key economic driver for their future;
- the system would be hugely expensive to set up and audit, and would require scientists and others to devote many hours to the review process;
- it is not intended to prevent malicious actors, and may thus be perceived as an unfair burden on legitimate science.

Finally, the outcomes of many, or even most, biology experiments cannot be determined ahead of time, making it difficult to prevent the formation of dual-use knowledge. If it were possible to know these outcomes, there would be no need to do the experiments. Any mechanism that attempts to deal with potentially dangerous knowledge will have to contend with possible side effects on legitimate, and potentially life-saving, research.

While the debate about how to best deal with dual-use dangers continues, scientists and policy makers should take care of the obvious threats. They should

also focus on health and safety by being better equipped to respond to infectious diseases. Considering all we know about anthrax disease, and the fact that *Bacillus anthracis* was used in a biological weapons attack seven years ago, it is deeply disturbing that the United States is ill prepared to respond to an aerosol anthrax attack. If we can't respond adequately, if there isn't enough vaccine, and if people can't get antibiotics fast enough to make a difference, it will still be an attractive weapon.

## The best security measure is transparency

IRIS HUNGER | 24 JANUARY 2008

Two more thoughts on the issue of expertise: Expertise is important in building a bioweapon, but there are different types of expertise. As Jens Kuhn says, expertise in weaponization is rare. Expertise in synthesizing certain viruses is not. In talking about access to expertise we therefore need to clarify which expertise we mean.

Answering Gigi Kwik Gronvall's first set of questions: Of course, one of a thousand scientists can be bought, and there is no proof that none of the Russian bioweapons experts has moved to a country of concern. The point, however, is that it would seem to be a very rare event. Finding the one scientist among thousands that would be willing and able to work on bioweapons requires time and resources. This slows bioweapons efforts down and increases the chance of uncovering them before they are "successful."

The same basic argument is true regarding Gigi's second set of questions. Of course, terrorists can learn through trial and error and generate the necessary knowledge on their own. But again, this is time and resource consuming. We can hope to make the path to a bioweapon longer and more complicated, but it is impossible to ensure 100 percent prevention.

Gigi invited comments on the specific proposals that have been put forward. Before commenting on those specific proposals, I would like to say something general: What we need is transparency, and transparency efforts need to focus on the areas of greatest concern. Only then are we likely to uncover noncompliance. How do you define what activities are of greatest concern? In general, the more dangerous the agents being researched and the closer the work moves toward weaponization, the greater our concern should be.

With this basic thought in mind, the three measures Gigi listed are of limited usefullness, at least if they are not appropriately focused. Jens eloquently described the problems associated with screening gene sequence orders for dangerous sequences. Such screening could be useful in cases where a suspicion already exists, or for very specific sequences, such as parts of the smallpox genome. I agree with Gigi that requiring companies to store their sequence orders would be a minimal burden, and the data could be left untouched unless an investigation becomes necessary, i.e. a suspicion requires following up on a sequence order. I could also imagine using data-mining software to anonymously check sequence orders for suspicious aggregations of dangerous sequences,

though I don't know how much this would add to our knowledge of what is being done with sequence data and gene sequences. Do the other discussants have thoughts about this?

Regarding the licensing of scientists, I am not sure that I understand the proposal. In Germany, and I believe all over Europe, scientists working in high or maximum containment facilities receive extensive safety training. What would licensing add, unless licensing were obligatory on a global scale?

## Stopping dangerous research before it starts

JENS H. KUHN | 18 JANUARY 2008

This discussion needs some clarification. Iris Hunger is right in stating that the expertise to build and deploy a biological weapon is distributed among only a few people who are difficult (but not impossible) to recruit. However, so far, this discussion has focused on what can be done with available sequence *information*, i.e. constructing a pathogen using these data. As I have pointed out, the synthesis of certain viruses is not laborious or technically difficult, nor does it require extensive training. Thankfully, the remaining steps to a weapon (quantitative production, concentration, purification, stabilization, and dispersal) are much harder to accomplish.

I agree that a dedicated terrorist may find a way to get the information he or she wants, for example, by acquiring a pathogen and sequencing its genome--if genomic information is not publicly available. The question that should be steering this discussion is whether not-so-dedicated aggressors could easily utilize sequence information to synthesize pathogens. In my view, dedicated and financially supported terrorists would not need publicly available sequence information to begin a weapons program, and not-so-dedicated terrorists may manage to synthesize a pathogen only to get stuck in the weaponization process for which they would have to hire those hard-to-come-by experts. Therefore, I argue that the availability of natural pathogen sequences is not dangerous.

Iris did, however, raise an important point that has not been discussed as much as it deserves: "If it is likely that [scientists] will produce knowledge that they do not want to share with others, they simply should not produce it." Scientists have generated possibly dangerous genomes deliberately (e.g., the 1918 H1N1 influenza A virus) and by serendipity (e.g. the mousepox IL-4 virus). Both genomes do not occur in nature anymore. Should oversight systems have prevented these experiments, so as to not make sequences available that are not of direct public-health use? Should special rules apply to these experiments if they are performed, to restrict the public availability of such sequences?

The concept that there might be some information not worth knowing is anathema to scientists, but research decisions are based on many different considerations. Scientists try to fit their research into the prevailing funding environment so that it can be seen as consistent with national priorities. Many scientific questions that would generate new information are thus left unanswered, due to either lack of

expected scientific merit, potential for publication, or, most often, available financial support. This leads me to question whether funding authorities and scientists who construct novel pathogens, and thereby increase the risk that terrorists repeat the same experiments with malevolent goals, have their priorities always straight.

To begin addressing these issues, I think that scientists and policy experts should work together to install an oversight system akin to that proposed by the Center for International and Security Studies at Maryland that evaluates, accepts, rejects, or modifies proposed scientific projects with potential high-risk outcomes *before* any such research is carried out. There should be consensus that a research project is important before it ensues, i.e. the public-health benefit outweighs the risks. This way, as Iris says, once an experiment is performed, its findings can be published in full.

As I pointed out before, I don't think that screening oligonucleotide orders will be useful at this time because the process is likely to generate too many false-positive alarms. We already established that the synthesis of pathogens can be done only by scientists, so licensing scientists would be of questionable benefit, since terrorists would then simply hire a licensed scientist.

## Which control mechanisms will work?

GIGI KWIK GRONVALL | 9 JANUARY 2008

I strongly disagree with Iris Hunger's assertion that history teaches us that biological expertise can't be purchased. One obvious counterargument is that history is full of achievements that were thought to be unlikely, even impossible, that is, until someone proved otherwise. This is particularly the case in the realm of inventions (and weapons) stemming from scientific advancements. But there is also the matter of proof: While most former bioweapons scientists may not have switched allegiances for money, is there evidence that *none* of them have? What about ordinary scientists who had no ties to bioweapons programs--is it possible that not one of thousands of scientists could be bought?

I also wonder about how truly important the tacit knowledge of weaponization is to a prospective bioweaponeer. Could direct information from a bioweapons program help a trained scientist design a weapon? I have no doubt that it could. But could the lack of direct experience be overcome with trial and error, a background in laboratory work, and perhaps knowledge gleaned from everyday biological controls (such as spraying certain bacteria on crops to repel insects) or biologics pharmaceutical manufacturing? It seems foolhardy to bet otherwise. After all, people who have made bioweapons had to learn at some point, and presumably, technological advances in biology have made that learning curve less steep.

In this round of comments, I would like to hear what my fellow discussants think about several specific proposed control mechanisms for science. Some have been taken from the "Synthetic Genomics: Options for Governance" report I mentioned in a previous comment. I invite my fellow discussants to suggest additional methods that they would either consider or reject to control the misuse of scientific research:

- requiring gene firms or oligonucleotide manufacturers to screen orders for potentially dangerous sequences;
- requiring gene firms or oligonucleotide manufacturers to store their orders, in case attribution becomes necessary;
- requiring licensing of those who order sequences from gene firms or oligonucleotide manufacturers, or requiring licensing scientists more generally.

Screening orders for potentially dangerous sequences is technically possible, and could prevent or mitigate an attack. However, it would be very important to establish what would be done if a suspicious sequence is detected, and if further investigation reveals that it was ordered by a researcher who has no obvious reason to order the sequence. I don't think it would be useful to involve the FBI for every sequence order that seems suspect, particularly as judgments are unlikely to be cut and dry. It would also be important to minimize the burden on the private companies that would be responsible for screening orders and reporting them; screening would be done at a cost, and in a global marketplace, it could place firms at a competitive disadvantage. Similarly, a reporting structure would need to minimize the burden on the company. For example, it may prove more advantageous to not report if the firm is shut down while an investigation commences. If those measures are in place, requiring gene firms to store their orders appears to be a minimal burden, and could help in an investigation.

I have sympathy with those who think that every scientist in a lab should be licensed, because many professions require licensing, and why should science be different? For example, engineers, electricians, hair stylists, and manicurists require a license to work. I also understand the rationale of scientists who oppose this concept and point to the degree on their wall and say, "See this PhD? This is my license." In the end, however, I think that a licensing regime would be very expensive and should be reserved for work in Biosafety Level-3 and Biosafety Level-4 laboratories. In this high-containment environment, researchers have access to, and have the potential to be exposed to diseases that may be immediate public health dangers. The public relies on these scientists to handle biological agents safely. A licensing regime may help to ensure that, at the very least, these workers receive safety training. I look forward to hearing others' opinions!

## The danger is too great to allow unrestricted access

LEONID F. RYABIKHIN | 3 JANUARY 2008

There appears to be some consensus. As Iris Hunger wrote: "Is the availability of genetic information dangerous? Certainly."

Our lives are full of threats and dangers. But each threat differs from the others and ranges from minimally to extremely dangerous. Humans typically elaborate rules and regulations to secure people and the environment from extremely negative consequences. We have driving safety, flight safety, and many other examples of "safeties." Yet, it is hard to compare driving safety with biosafety. Humans have coexisted and fought with microbes since their very beginning. Thus, biosafety

became one of the highest priorities for human survival, and we continue to develop measures to protect ourselves from the huge variety of biothreats.

States and scientists have attempted to provide for the physical and biological security of dangerous pathogens. The absence of large-scale bioattacks and the lack of evidence that terrorists possess biological weapons are positive results of such measures. But we should not underestimate the possible malevolent use of any of the diverse pathogens existing in nature or the engineering of pathogens in laboratories.

Establishing a set of rules and procedures for regulating and controlling access to genetic information will help to create a compromise between free access to genetic information and security needs. Iris Hunger introduced some ideas, but this problem needs broader and deeper consideration by life scientists and security experts.

In the meantime, I would like to echo Gigi Kwik Gronvall's call for hospital readiness and the rapid production of medical countermeasures. National health care systems must have highly effective response measures in place to use against existing and emerging infectious diseases of natural character. Such systems will also work against deliberate bioattacks.

## The case for preventive measures

IRIS HUNGER | 26 DECEMBER 2007

My fellow discussants repeatedly allude to the same reason to explain why we need to keep sequence data public: Not doing so would harm the advancement of science and would prevent the development of top-quality medicine, including for biodefense purposes. This implies that they would limit the availability of this information, were it not for this "do no harm to science" rule. I would argue, instead, that limits are inappropriate because, quite simply, they do not work. They will not prevent access: A dedicated terrorist will find a way to get the information he or she wants. But even if limits prevented access, they would not remove the threat. If we remove sequence data for traditional biological weapons agents such as smallpox from the public arena, who says that an enemy will not use regular influenza as a weapon? Plus, limits are not manageable globally. Who is to decide what information has to be limited? Who is and who is not allowed to have access to restricted information?

If scientists are serious about not wanting certain data available publicly, they need to think before they act. If it is likely that they will produce knowledge that they do not want to share with others, they simply should not produce it. The concept is preventive arms control. Scientists have to ask themselves whether it is worth it to take certain paths of research. In other words, they need to make a risk-benefit assessment before starting a project. Once a research project has been conducted, it should be published in full.

On a second point: the price of expertise. Both Gigi Gronvall and Jens Kuhn say

that expertise can be bought, and therefore it is not a serious limiting factor in bioweapons development. History, however, teaches otherwise. The Japanese cult Aum Shinrikyo had trained scientists and a lot of money, and they did not successfully create a bioweapon. Al Qaeda certainly has a lot of money. In the past, they could convince a PhD-level Pakistani microbiologist to provide them with information, but tacit knowledge was not for sale. Other experts that could be bought, such as bioweapons experts from the former Soviet Union, are also not for hire. Most of them are in Western research projects--mostly civilian--not in Iran, Syria, or North Korea.

Lastly, both Leonid Ryabikhin and Jens Kuhn ask to "continue to explore possible ways to control bioinformation" and to "broaden our thinking." Well, do it! Please! I would like to hear new ideas; it does not seem to be easy. There is a lack of innovation about how to control the use of the diversified, globalized, and dual-use technologies, equipment, and knowledge in the life sciences.

In my view, a key principle has to be that we do not try to prevent certain activities from happening, but that we simply watch what people do. If someone or some country is engaged in a suspicious activity that might indicate bioweapon development--and this will be rare--governments and civil society should ask questions about intentions, whether the suspicious activities are taking place in the United States, Germany, Iran, or Malawi; or whether they are taking place in government, industry, or military facilities.

Scientists and governments need to be able to enter into a proper dialogue about these types of activities. Knowing that a gene synthesizer is located somewhere tells you about capabilities, but only through dialogue will we be able to determine its intended use.

## Defining the terrorist risk

JENS H. KUHN | 18 DECEMBER 2007

The participants of this roundtable, including myself, agree that it is a bad idea to limit access to pathogen sequence information. However, we seem to disagree on *why* we agree. Iris Hunger wrote that it is unlikely that available sequences will be misused by terrorists because gene synthesis requires tacit knowledge. But what do we mean by "terrorist"?

While I agree that the role of tacit knowledge in the creation of biological weapons is very important and frequently overlooked, I also agree with Gigi Kwik Gronvall that its importance diminishes if we assume that a terrorist group either has the means to hire trained scientists or that it consists of scientists. Additionally, one does not need modern gene synthesis technology to create the genomes of many viral agents: standard recursive polymerase chain reaction will suffice and has been around for many years. (For example, the first reported creation of a pathogen, the *in-vitro* synthesis of a poliovirus, was not based on a novel scientific method. At the time, scientists were using more efficient and much faster ways to create large complementary DNA blocks based on sequence information. Eckard Wimmer's

poliovirus publication was simply a proof-of-concept project.)

Many priority pathogens have simple and short genomes, which themselves are infectious. The methods to create these genomes are so standard that they are not even described in the method sections of publications anymore. This means that the tacit knowledge to apply these methods is widely spread and practically speaking "for hire."

Other agents require more sophistication. The genomes of negative-stranded RNA viruses, for instance the Zaire ebolavirus or 1918 H1N1 influenza A virus, are not infectious by themselves, but require the presence of viral helper proteins, which also have to be synthesized and present inside of a cell in the right numbers. It takes longer to create such reverse genetic systems, and a limited number of people have the skill to succeed, but the methods themselves are not any different from those routinely used by thousands of scientists and taught to students within months. Also, scientists have already created and published many RNA viruses of concern, using individual sequences obtained separately--not synthesized. Other agents, such as the variola virus and bacteria are not within reach of individuals, because the methods to synthesize them are not as widely distributed or not yet developed.

Tacit knowledge becomes particularly important for the steps after the synthesis of a virus, as Leonid Ryabikhin asserts. The methods to stabilize, coat, store, and disperse a biological agent are highly complicated, known only to a few people, and rarely published. I am not too concerned about publicly available pathogen sequences--not because I think people can't misuse them to synthesize an agent, but because if they chose to do so and succeed they will in all likelihood get stuck during the weaponization process. Meanwhile, the scientific community uses pathogen sequences to gain tremendously important information about creating countermeasures against all kinds of threats.

Hunger's suggestion to control the work based on publicly available sequences merits further discussion. It is often suggested that companies offering gene synthesis should screen for "dangerous" sequences. But how would such "dangerous" sequences be defined and who would establish the definitions? It would be counterproductive for ordinary infectious disease research to ring alarm bells any time scientists order a piece of a Priority Pathogen genome. Entire laboratories and institutes research individual genes or proteins of microbes without ever touching a "live" (replicating) agent. A company or, better, an outside oversight body would have to find a way to distinguish between these institutions' orders and those that might lead to the assembly of a complete pathogen genome.

How could this be achieved? And how would a decision be made to allow one "good" laboratory to assemble a genome, but not another? Are there other ways of controlling such work? Tracking the global distribution of gene-synthesizing equipment will only be a temporary solution, so we need to broaden our thinking.

## Is gene synthesis an "easy" technology?

GIGI KWIK GRONVALL | 5 DECEMBER 2007

The other participants in this roundtable have (rightly) focused not on the *access* to genetic sequence information, but what it is possible to *do* with that information. In one scenario, sequence information could be used to recreate pathogens from scratch, through gene synthesis technology. (A recent report, "Synthetic Genomics: Options for Governance," outlines three basic sets of policy options for dealing with the dark side of gene synthesis technology and gives the advantages and disadvantages of each course of action.)

I would like to pick up the topic by addressing a question that Jens Kuhn asked: "Is gene synthesis an 'easy' technology that, with the proper access to machinery and reagents, could truly be used by nonprofessionals (e.g. criminals and terrorists) to create microbial genomes in the nearest future? Or does the technology require a level of sophistication and financial support that will only be available to professionals?" Iris Hunger wrote that "it is not easy to synthesize a virus, not even for experts." And Leonid F. Ryabikhin wrote that developing bioweapons, in general, requires "a high-level of scientific and technological know-how. Numerous other obstacles make this task extremely complicated." The general feeling seems to be that biological weapons, particularly pathogens synthesized from scratch, are just too hard to make to be a real threat, particularly from individuals or small groups.

If that is the case, and the technical obstacles are in fact a good deterrent toward bioweapons development--terrific! But, frankly, I'm not that optimistic, and I believe that the urgency of the problem requires that much more be done to mitigate an attack, such as preparing hospitals and investing in more rapid production of medical countermeasures, etc.

Why don't I think that we can rest easy? Just a few reasons: Firstly, expertise can be bought. Al Qaeda apparently paid $1.5 million to acquire highly enriched uranium--thankfully, it turned out it was not as advertised. (For more information on this incident, please see this report.) But members of Al Qaeda thought they could purchase the expertise and the material required to create a nuclear device, and experts believe that this is feasible and worrying. In comparison, it would likely be less expensive to acquire the skills and reagents to build a biological weapon, even a pathogen synthesized from scratch.

Secondly, advanced technology will become more accessible. Before I went to graduate school, I worked as a lab technician, making short stretches of oligonucleotides for researchers at Memorial Sloan-Kettering Cancer Center. What I did, day in, day out, was very routine and required only a little training. But 10 years earlier synthesizing a short stretch of oligonucleotides could form the basis of a PhD thesis. An incredibly useful technology like gene synthesis will likely become accessible to the scientific masses even more rapidly--10 years from now, it is likely that it will be found in labs everywhere.

Thirdly, high levels of scientific sophistication can be found globally. Gene synthesis technology, and other complementing technologies that could be used to make a biological weapon, are not out of the range of biotech companies, research

institutions, and individual scientists in many parts of the world. Of course, it wouldn't be easy to make a biological weapon. But with persistence, it is doable, especially when the people doing the work are not breaking new scientific ground and know that it is physically possible that they can accomplish their goals.

I still think it is a good idea to keep sequence information freely available, because the benefits to security, to the development of medical countermeasures, and to scientific advancement outweigh the risks--but there *are* risks.

## Some biological information should be restricted

LEONID F. RYABIKHIN | 29 NOVEMBER 2007

Security experts, members of the arms control community, and bioscientists routinely name bioterrorism as one of the most challenging threats to national and international security. In my view, they have overestimated the potential use of biological agents by terrorist groups or irresponsible regimes.

Most states have no reason--political, military, nor economic--to unleash a bioweapons attack. Some regimes or states dream about possessing a means to deter aggressors and may consider obtaining bioweapons the easiest way to do this. But developing bioweapons is a difficult and sophisticated task, which requires a high-level of scientific and technological know-how. Numerous other obstacles make this task extremely complicated.

Speculation that an individual with limited scientific knowledge could make a dangerous bioagent in an ordinary kitchen does not reflect reality. The major bioterrorist is mother nature. Nations, public health authorities, and the scientific community must jointly build the robust biodefenses necessary to combat existing and emerging infectious disease outbreaks, both natural and intentional.

We can, however, reduce further the already low risk of deliberate bioattack. We need to strengthen the nonproliferation regime and work to improve implementation of the Biological and Toxin Weapons Convention. And the international community of bioscientists must work to prevent the misuse of advances in the life sciences, such as the ability to synthesize bioagents from scratch.

How do we do this? We can implement ethical norms, such as codes of conduct or laboratory best practices, and turn to law enforcement. But we also must think about how to control access to sensitive biological information, including the genetic information of organisms. I agree that we cannot close access to already available genetic information. Such information is vital and useful for constructing new drugs and vaccines against existing and newly emerging infectious diseases.

The international community and World Health Organization (in cooperation with other international organizations) have established and implemented international standards for the safe and secure handling of pathogens in diagnostic and research laboratories, in health care and pharmaceutical facilities, and in transport. The control of sensitive biological information must be integrated into these international biosafety rules and regulations.

Additionally, the dissemination of sensitive information in the life sciences has to be properly controlled, and access to some information must be restricted. Scientists and analysts must also be very cautious in discussing biosecurity problems publicly. In many forums, even in popular movies, an individual can find "useful" information to create panic and instability by misusing life science research for criminal or terrorist purposes. We need to continue to explore possible ways to control bioinformation.

## Secret biological research sets a bad precedent

IRIS HUNGER | 20 NOVEMBER 2007

Is the availability of genetic information dangerous? Certainly. But so is driving a car, flying to the moon, or falling in love. We do a lot of dangerous things, simply because the benefits outweigh our concerns.

So, how dangerous is it to have sequence data available? As Gigi Kwik Gronvall wrote, it is "potentially dangerous," i.e. there is the possibility for misuse. But how likely is the misuse by terrorists? I would argue, not very. Sequence data require knowledge and background information--or, as Cornell Professor Kathleen Vogel terms it "context"--to be translated into useful information.

Besides context, successful gene synthesis from sequence data requires tacit knowledge--the type of knowledge that is necessary to turn a recipe into a cake. Tacit knowledge is gained by repetition and often goes unnoticed because most people simply do things as they were taught to do them. The transfer of tacit knowledge requires long-term intensive contacts between people.

Keeping this in mind, I would argue that it is not easy to synthesize a virus, not even for experts. It would be even more difficult to create a bacterium from scratch. There are roads to developing a pathogen that are much easier to travel than gene synthesis, such as the ones alluded to by Jens Kuhn.

The other participants of this roundtable seem to share my view that sequence data should remain freely available. However, I sense some hesitation in their comments about whether certain very specific data such as sequences of eradicated diseases or artificial pathogens should be made public. This is a dangerous concept to entertain. Work on eradicated or artificial pathogens has a particularly high potential for misuse. If a state carried out such work and the results were kept hidden, suspicions would certainly arise among other states. Here, it is particularly useful to put yourself in the shoes of states that are not close allies. How would they interpret your behavior? If Russia, China, Iran, or India interpreted U.S. research of this sort as the first steps toward an offensive capacity, they would likely begin or increase their activities along the same lines.

If we agree that genetic data should remain freely available, what limits on the use of these data are useful and possible? Here are two possibilities: Companies that synthesize genetic sequences recently started to screen sequence orders for "dangerous" bits. The assumption is that suspicious aggregations of orders for

"dangerous" sequences, such as virulence factors or consecutive parts of the smallpox genome, would raise an alarm. This would make things more difficult for the "mid-level bad guy" who lacks the know-how and funds to synthesize sequences from scratch. Another option is to track the global distribution of certain equipment. If we knew, for instance, where all the high-speed gene synthetizers were located, we could keep a keen eye on how they were being used.

## Questions to consider about gene synthesis technology

JENS H. KUHN | 13 NOVEMBER 2007

Microbiological research is increasingly troubled by ethical questions regarding its potential misuse. In the near future, a criminal, terrorist, or state seeking to build a bioweapon might choose to obtain a pathogen by synthesizing it *in vitro* and changing its properties, instead of isolating it from nature or stealing it from maximum-containment facilities. Numerous logistical and technological obstacles complicate the construction and release of a bioweapon, but the first step--obtaining a suitable agent through clandestine synthesis--is becoming a realistic scenario that needs to be addressed by scientists and the arms control community.

In the past, *in-vitro* synthesis of biological agents was restricted to viruses with small infectious genomes that not only had to be sequenced fully but also had to be physically available as templates. In 2002, researchers at SUNY Stony Brook first demonstrated that a template genome was not necessary to create a poliovirus from scratch. Over a two-year time period, this group assembled the genome using short overlapping oligonucleotides designed according to the published poliovirus genome sequence and ordered through a commercial supplier. Similar experiments in 2003 yielded an encephalomyocarditis virus.

The newest technology on the market, fittingly named gene synthesis, combines microfluidic chip technology, one-step polymerase chain reaction assembly, and a novel assembly technique to accurately create large nucleotide building blocks that can later be joined. By using these new techniques in combination with standard molecular biology, it will be feasible to synthesize genomes the size of all known viruses and bacteria *in vitro*.

Limiting access to the sequence information on which the design of genomes is based could control what is synthesized, but would the costs be worth the benefits? Addressing the following questions would help to understand this larger issue:

- Is gene synthesis an "easy" technology that, with the proper access to machinery and reagents, could truly be used by nonprofessionals (e.g. criminals and terrorists) to create microbial genomes in the nearest future? Or does the technology require a level of sophistication and financial support that will only be available to professionals?
- Would limited access to pathogen sequences impede scientists' ability to develop countermeasures against these agents?
- Who would decide to withhold or withdraw sequence information, and according to which criteria would decision makers allow individuals or

organizations to access otherwise unavailable sequences?

- How much would we actually gain by withholding sequence information? Aren't technologically advanced aggressors, such as nation states, able to obtain natural organisms and then sequence their genomes? Wouldn't technologically advanced aggressors, such as nation states, prefer to obtain their own sequences? If technologically advanced aggressors can obtain natural organisms, what need would they have for sequence databases, and what implications would this have for any effort to control sequence information?
- Should access to sequences from eradicated pathogens or artificial microbes be limited? If the public-health concern is considered grave enough to retain eradicated viruses or to resurrect them, shouldn't information about them be publicly available?
- If a nation chose to withdraw existing, publicly available sequences, is it possible to ensure that other nations not grow suspicious of its motives? Is it even feasible to withdraw previously available information from the public?
- What is the overlap between "bioweapons agents" and "public health agents"? Couldn't an aggressor turn those agents into weapons that we consider non-bioweapons agents and for which sequence information would remain publicly available?

## Access leads to better science, and better security

GIGI KWIK GRONVALL | 8 NOVEMBER 2007

Point your web browser to the National Center for Biotechnology Information (NCBI), and you will find a treasure trove of genetic information. No fee or password is required to copy and paste the genetic code for Ebola Zaire, one of the most lethal strains of the Ebola virus, or variola, the virus that causes smallpox. According to the NCBI website, sequences of more than 130 billion base pairs (the building blocks for DNA) were available in April 2006, and the amount is expanding exponentially over time.

Is this widespread availability of genetic information a problem? It certainly could be. In the hands of a biologist intending to cause harm, the sequence information available on the internet could be the first step in bringing back the 1918 flu virus, for example. Alternatively, someone could make a currently circulating virus, such as Ebola, without getting the virus from a laboratory or an ongoing outbreak. With a detailed road map, they could construct it using chemical reagents and widely available technology. DNA synthesis technologies are getting better and faster, enabling greater swaths of genetic material to be more accurately produced.

Yet, should anything be done about these freely available sequences of potentially dangerous information? In my opinion, no. There are two main reasons why. Firstly, the information is already out there, and it is difficult to take something back in the digital age. But this begs the question, is there any genetic sequence that one can imagine that has not yet been posted that should *not* be freely accessible?

Secondly, the information is useful. For example, Siga Technologies's

investigational new drug ST-246 was developed through an examination of the genetic sequences of poxviruses, including smallpox. The drug inhibits a protein essential for virus assembly, a protein found in multiple poxviruses but not in humans. This drug was successfully used to treat a boy who had developed eczema vaccinatum, a rare but serious complication of the smallpox vaccine that causes skin rashes in people with skin conditions such as eczema or atopic dermatitis. The boy had been exposed to the vaccine, which is a live virus, from contact with his father, who had been vaccinated against smallpox before deployment to Iraq.

Could all of this genetic information be available to those who could use it wisely, without letting *everyone* see? Not likely. It is difficult to imagine how one would decide who is allowed access, considering that the pursuit of biological sciences (and drugs and vaccines) is global. The information is needed in both the public and private sectors. If one were to block certain pathogens from access, it wouldn't help those who might be interested in developing countermeasures against them. Blocking access to agents that could be used as weapons would also isolate the biodefense research community, which would not be good for the quality of the science. Given the serendipitous nature of biology, blocking sequences could block scientists from understanding the significance of their work.

The question of whether genetic information for pathogens should be accessible has been considered by the National Research Council, in their report "Seeking Security: Pathogens, Open Access, and Genome Databases." They came to the conclusion that the current open access policy should not change, and that it is not practical or productive to block access. They recommend--and I strongly agree--that genetic information should be exploited fully to defend against infectious diseases of all types, whether they occur naturally or are the result of bioterrorism. Scientists should also be aware that misuse of this information is possible, perhaps even likely, and that defeating these bugs (and the misuse of them) will only happen through their efforts.