research in the United States has raised questions and national level.

Finally, the specter of classifying or controlling life sciences research raises larger security issues. The post-2001 expansion of biodefense research in the United States has raised questions as to whether the U.S. effort was in violation of the international BWTC (15). One of our strongest arguments against this perception is the openness of the university environment in which much of this research takes place, a transparent system that helps dispel concerns of a “secret” U.S. bioweapons program. Classifying the research, redacting research results, or driving select agent research out of universities to national or defense laboratories will only exacerbate this negative perception of the U.S. life science research program, which could cause greater national security or diplomatic issues. We have already seen this concern play out in the H5N1 publications case, as NSABB Acting Chair Paul Keim recently testified at a Senate Homeland Security and Government Affairs Committee hearing (16).

Is There a Better Path Forward?
The life sciences and security communities represent two perspectives with one common goal of working for the public good. It is unfortunate that the controversy over the H5N1 publications has in some cases polarized what has been an evolving and productive discussion, nationally and internationally, on how to work together to foster the highest-quality, appropriately regulated biological research (1).

Reaching that goal will require balance, which in this context can perhaps be best defined as the understanding that the most stringent security measures do not necessarily translate to a commensurate increase in security, nor does scientific freedom equate to abrogation of responsibility. It has already been demonstrated that scientists, once made aware of the potential risks associated with their research, are willing to modify their research methodologies or communications to minimize the risk (17).

The proposed modification to the Select Agent Rule adds additional requirements for biosafety and biosecurity training for those personnel with any access to these dangerous pathogens (4). Although institutions conducting research with select agents or in biocontainment laboratories already typically conduct extensive training of personnel, it does not seem unreasonable to add a discussion of the risks of dual-use research as a component of that required training. There are already a number of excellent resources for DURC education available, including modules developed by the NSABB (18) and the Federation of American Scientists (5), both at the local and national level.

Finally, responsible communication of research should start with the principles set forth by the NSABB. These include consideration of “the need for the inclusion of contextual and explanatory information that might minimize” concerns about the dangers posed by the research; an examination of the protective and oversight measures currently in place; and a full understanding and analysis of the positive benefit of the study (19).

References
16. P. Keim, Testimony of Paul Keim to the Senate Homeland Security and Government Affairs Committee, 26 April 2012; www.hsgac.senate.gov/download/?id=4c7bd5ae-9ca4-4b53-9c7c-59e25626f546.

PERSPECTIVE

Securing Medical Research: A Cybersecurity Point of View

Bruce Schneier

The problem of securing biological research data is a difficult and complicated one. Our ability to secure data on computers is not robust enough to ensure the security of existing data sets. Lessons from cryptography illustrate that neither secrecy measures, such as deleting technical details, nor national solutions, such as export controls, will work.

Science and Nature have each published papers on the H5N1 virus in humans after considerable debate about whether the research results in those papers could help terrorists create a bioweapon (1, 2). This notion of “dual use” research is an important one for the community, and one that will sooner or later become critical. Perhaps these two papers are not dangerous in the wrong hands, but eventually there will be research results that are.

My background is in cryptography and computer security. I cannot comment on the potential value or harm from any particular piece of biological research, but I can discuss what works and what does not to keep research data secure. The cryptography and computer security community have been wrestling for decades now with dual-use research: for example, whether to publish new Windows (Microsoft Corporation) vulnerabilities that can be immediately used to attack computers but whose publication helps us make the operating system more secure in the long run. From this experience, I offer five points to the virology community.

First, security based on secrecy is inherently fragile. The more secrets a system has, the less secure it is. A door lock that has a secret but unchangedable locking mechanism is less secure than a commercially purchased door lock with an easily changeable key. In cryptography, this is known as Kerckhoffs’ principle: Put all your secrecy into the key and none into the cryptographic algorithm (3, 4). The key is unique and easily changeable; the algorithm is system-wide and much more likely to become public. In fact,

 Minneapolis, MN 55410, USA. E-mail: schneier@schneier.com

www.sciencemag.org SCIENCE VOL 336 22 JUNE 2012 1527
algorithms are deliberately published so that they get analyzed broadly. The lesson for dual-use virology research is that it is risky to base your security on keeping research secret. Militaries spend an enormous amount of money trying to maintain secret research laboratories, and even they do not always get security right. Once secret data become public, there is no way to go back.

Second, omitting technical details from published research is a poor security measure. We tried this in computer security with regard to vulnerabilities, announcing general information but not publishing specifics. The problem is that once the general information is announced, it is much easier for another researcher to replicate the results and generate the details. This is probably even more true in virology research than in computer security research, where the very existence of a result can provide much of the road map to that result.

Third, technical difficulty as a security measure has only short-term value. Technology only gets better; it never gets worse. To believe that some research cannot be replicated by amateurs because it requires equipment only available to state-of-the-art research institutions is short-sighted at best. What is impossible today will be a Ph.D. thesis in 20 years, and what was a Ph.D. thesis 20 years ago is a high-school science fair project today.

Fourth, securing research data in computer networks is risky at best. If you read newspapers, you know the current state of the art in computer security: Everything gets hacked. Cyber criminals steal money from banks. Cyber spies steal data from military computers. Although people talk about H5N1 research in terms of securing the research papers, that is largely a red herring; even if no papers existed, the research data would still be on a network-connected computer somewhere.

Not all computers are hacked and not all data gets stolen, but the risks are there. There are two basic types of threats in cyberspace. There are the opportunists: for example, criminals who want to break into a retail merchant’s system and steal a thousand credit card numbers. Against these attackers, relative security is what matters. Because the criminals do not care whom they attack, you are safe if you are more secure than other networks. The other type of threat is a targeted attack. These are attackers who, for whatever reason, want to attack a particular network. The buzzword in Internet security for this is “advanced persistent threat” (5). It is almost impossible to secure a network against a sufficiently skilled and tenacious adversary. All we can do is make the attacker’s job harder.

This does not mean that all virology data will be stolen via computer networks, but it does mean that, once the existence of that data becomes public knowledge, you should assume that the bad guys will be able to get their hands on it.

Lastly, national measures that prohibit publication will not work in an international community, especially in the Internet age. If either Science or Nature had refused to publish the H5N1 papers, they would have been published somewhere else. Even if some countries stop funding—or ban—this sort of research, it will still happen in another country.

The U.S. cryptography community saw this in the 1970s and early 1980s. At that time, the National Security Agency (NSA) controlled cryptography research, which included denying funding for research, classifying results after the fact, and using export-control laws to limit what ended up in products. This was the pre-Internet world, and it worked for a while. In the 1980s they gave up on classifying research, because an international community arose (6). The limited ability for U.S. researchers to get funding for block-cipher cryptanalysis merely moved that research to Europe and Asia. The NSA continued to limit the spread of cryptography via export-control laws; the U.S.-centric nature of the computer industry meant that this was effective. In the 1990s they gave up on controlling software because the international online community became mainstream; this period was called “the Crypto Wars” (7). Export-control laws did prevent Microsoft from embedding cryptography into Windows for over a decade, but it did nothing to prevent products made in other countries from filling the market gaps.

Today, there are no restrictions on cryptography, and many U.S. government standards are the result of public international competitions. Right now the National Institute of Standards and Technology is working on a new Secure Hash Algorithm standard (8). When it is announced next year, it will be the product of a public call for algorithms that resulted in 64 submissions from over a dozen countries and then years of international analysis. The practical effects of unrestricted research are seen in the computer security you use today: on your computer, as you browse the Internet and engage in commerce, and on your cell phone and other smart devices. Sure, the bad guys make use of this research, too, but the beneficial uses far outweigh the malicious ones.

The computer security community has also had to wrestle with these dual-use issues. In the early days of public computing, researchers who discovered vulnerabilities would quietly tell the product vendors so as to not also alert hackers. But all too often, the vendors would ignore the researchers. Because the vulnerability was not public, there was no urgency to fix it. Fixes might go into the next product release. Researchers, tired of this, started publishing the existence of vulnerabilities but not the details. Vendors, in response, tried to muzzle the researchers. They threatened them with lawsuits and belittled them in the press, calling the vulnerabilities only theoretical and not practical. The response from the researchers was predictable: They started publishing full details, and sometimes even code, demonstrating the vulnerabilities they found. This was called “full disclosure” and is the primary reason vendors now patch vulnerabilities quickly (9). Faced with published vulnerabilities that they could not pretend did not exist and that the hackers could use, they started building internal procedures to quickly issue patches. If you use Microsoft Windows, you know about “patch Tuesday,” the once-a-month automatic download and installation of security patches.

Once vendors started taking security patches seriously, the research community (university researchers, security consultants, and informal hackers) moved to something called “responsible disclosure.” Now it is common for researchers to alert vendors before publication, giving them a month or two head start to release a security patch. But without the threat of full disclosure, responsible disclosure would not work, and vendors would go back to ignoring security vulnerabilities (10, 11).

Could a similar process work for viruses? That is, could the makers work in concert with people who develop vaccines so that vaccines become available at the same time as the original results are released? Certainly this is not easy in practice, but perhaps it is a goal to work toward.

Limiting research, either through government classification or legal threats from vendors, has a chilling effect. Why would professors or graduate students choose cryptography or computer security if they were going to be prevented from publishing their results? Once these sorts of research slow down, the increasing ignorance hurts us all.

On the other hand, the current vibrant fields of cryptography and computer security are a direct result of our willingness to publish methods of attack. Making and breaking systems are one and the same; you cannot learn one without the other. (Some universities even offer classes in computer virus writing.) Cryptography is better, and computers and networks are more secure, because our communities openly publish details on how to attack systems.

Virology is not computer science. A biological virus is not the same as a computer virus. A
vulnerability that affects every individual copy of Windows is not as bad as a vulnerability that affects every individual person. Still, the lessons from computer security are valuable to anyone considering policies intended to encourage life-saving research in virology while at the same time prevent that research from being used to cause harm. This debate will not go away; it will only get more urgent.

References and Notes
1. M. Imai et al., Nature; published online 2 May 2012, 10.1038/nature10831.

POLICY FORUM

Evolution, Safety, and Highly Pathogenic Influenza Viruses
Marc Lipsitch, 1,2,* Joshua B. Plotkin, 3 Lone Simonsen, 4 Barry Bloom 2

Experience with influenza has shown that predictions of virus phenotype or fitness from nucleotide sequence are imperfect and that predicting the timing and course of evolution is extremely difficult. Such uncertainty means that the risk of experiments with mammalian-transmissible, possibly highly virulent influenza viruses remains high even if some aspects of their laboratory biology are reassuring; it also implies limitations on the ability of laboratory observations to guide interpretation of surveillance of strains in the field. Thus, we propose that future experiments with virulent pathogens whose accidental or deliberate release could lead to extensive spread in human populations should be limited by explicit risk-benefit considerations.

In response to two sets of experiments on mammalian-transmissible, modified influenza A/H5N1 viruses (1, 2) the U.S. Department of Health and Human Services has promulgated a new policy on dual-use research of concern (3). This policy, and other statements from U.S. and international bodies, identify the need for risk mitigation in future studies of mammalian-transmissible variants of highly pathogenic influenza virus and certain other infectious agents (4, 5), raising an important new question: How should funders, regulators, and researchers evaluate what future experiments should be done with such viruses? The answer to this question depends on the relative magnitude of risks and benefits of such experiments. For influenza, useful evaluations of either risks or benefits depend in part on what we know about virus evolution. Proponents of continued research in this area suggest that knowing the mutations involved in mammalian airborne transmission will aid surveillance, allowing us to see whether there is evolution in the direction of a pandemic virus. Mitigating the risk of accidental or deliberate release of these strains, as directed by the new policy (3), also depends on how well we can predict the virulence, transmissibility, and evolutionary trajectory of influenza viruses.

We contend that predictions about how particular influenza strains will behave in humans or, even more important, how they will evolve, remain highly speculative. The most striking examples of influenza’s unpredictability are in the area of drug resistance. Animal models, in vitro studies, and mathematical models have all contributed to our understanding of drug-resistant strains. Despite that knowledge, aspects of the spread of adamantane-resistant A/H3N2 (2003 to the present) and the spread of oseltamivir-resistant A/H1N1 (2007 to 2009) took the influenza community by surprise.

Adamantanes were used to treat influenza starting in the late 1960s. Animal models showed essentially no “fitness cost” or virulence reduction in strains with mutations conferring adamantane resistance (6), which commonly emerge during treatment (7) and can spread within families (7). These observations would have predicted a high likelihood that adamantane resistance would spread widely in populations where adamantanes were used, but such spread did not occur for decades, for reasons that remain unclear. Then, in 2003 to 2004, adamantane-resistant viruses emerged to rapidly become the dominant influenza A/H3N2 isolates globally (8, 9). Although adamantane use likely played a role in the genesis and initial spread of the resistant lineage (8), the near-fixation of this lineage in global A/H3N2 isolates may have been due to the presence of immune escape mutations (9), a selection pressure whose importance in spreading this virus could not have been confidently predicted. Also unanticipated was the persistence of resistant viruses to the present day, despite minimal use of adamantanes (9).

Resistant strains emerge de novo in several percent of influenza patients treated with the neuraminidase inhibitor oseltamivir (10). However, extensive spread of resistance was not reported before 2007. At the time, this situation was explainable by the large fitness costs observed in animal models for the most common oseltamivir-resistance mutation (11). Preclinical and effectiveness trials showed resistance in 5 to 10% of patients treated with oseltamivir, and the frequency of resistance increased with time on treatment. However, we know little about the frequency and speed of emergence of drug-resistant strains in communities. Many of the factors affecting the spread of drug-resistant strains in humans are also important in the spread of drug-resistant bacterial strains, and the mechanisms for transmission and persistence of drug resistance in human populations are implicit in our understanding of the spread of drug-resistant bacterial strains.


12. This article was based on a talk given at the meeting HSAN Research, Biosecurity, Biosecurity, and Bioethics, Royal Society, London, 3 April 2012.

10.1126/science.1224321

1. Center for Communicable Disease Dynamics and Department of Epidemiology, Harvard School of Public Health, Boston, MA 02115, USA. 2. Department of Immunology and Infectious Diseases, Harvard School of Public Health, Boston, MA 02115, USA. 3. Department of Biology, University of Pennsylvania, Philadelphia, PA 19104, USA. 4. Department of Global Health, George Washington University School of Public Health and Health Services, Washington, DC 20037, USA.

*To whom correspondence should be addressed. E-mail: milips@hsph.harvard.edu

5. M. K. Daly, presentation at the 23rd Large Installation System Administration (LISA) Conference, Baltimore, MD, 4 November 2009.
Editor's Summary

This copy is for your personal, non-commercial use only.

**Article Tools**  
Visit the online version of this article to access the personalization and article tools:  
http://science.sciencemag.org/content/336/6088/1527

**Permissions**  
Obtain information about reproducing this article:  
http://www.sciencemag.org/about/permissions.dtl