FOREIGN AFFAIRS

MAY/JUNE 2002

Toward Biological Security

Christopher F. Chyba

Volume 81 • Number 3

Toward Biological Security

Christopher F. Chyba

MISPLACED ANALOGIES

THE ANTHRAX ATTACKS on the United States in the autumn of 2001, and the fear and confusion that followed, made clear that the country lacks a comprehensive strategy for biological security—the protection of people and agriculture against disease threats, whether from biological weapons or natural outbreaks. Too often, thinking about biological security has been distorted by misplaced analogies to nuclear or chemical weapons. An effective strategy must leave these analogies largely behind and address the special challenges posed by biological threats.

A strategy for biological security must confront drug-resistant and emerging diseases—more than 30 of which have entered the human population over the past quarter-century. There is no good analogue to this naturally occurring threat in the realm of nuclear or chemical weapons. Moreover, diseases may be targeted against livestock or crops as well as against human populations. And outbreaks of deadly, contagious, and long-incubating diseases such as smallpox have to be detected and stopped rapidly wherever in the world they occur. Fortunately, once formulated, a sound strategy for biological security will help sustain itself because many of its core provisions will benefit public health even apart from acts of bioterror.

In fact, many of the tools used to address natural disease threats will be needed to respond to an intentional attack. The U.S. response to the anthrax attacks has emphasized the importance of improving

---

CHRISTOPHER F. CHYBA is Codirector of Stanford University's Center for International Security and Cooperation and holds the Carl Sagan Chair for the Study of Life in the Universe at the SETI Institute. He served on the staff of the National Security Council in the Clinton administration.

domestic defenses. These measures include stockpiling vaccines and antibiotics, as well as improving local and national disease surveillance and other public health tools. To be effective these domestic measures must be sustained for decades and keep pace with the biotechnology revolution. International steps—such as improving surveillance for and response to outbreaks of infectious diseases and securing pathogen stocks worldwide—are also crucial to an effective strategy. Yet most of these international measures have been ignored so far in the current focus on immediate domestic needs.

Part of the problem is the very vocabulary we use. Analysts and policymakers refer casually to "WMD" (weapons of mass destruction) or "NBCR" (nuclear/biological/chemical/radiological) weapons, as if the latter were merely variants on the same type of device. In fact, these weapons differ greatly in their ease of production, in the challenges they pose for deterrence, and in the effectiveness of defensive measures against them. The post–September 11 focus on WMD and whether they are in the hands of enemy states or groups risks overlooking these complexities. Put simply, biological weapons differ from nuclear or chemical weapons, and any biological security strategy should begin by paying attention to these differences.

THE WMD CONTINUUM

IMAGINE a line that begins with nuclear weapons at one extreme, continues through chemical, radiological, and biological weapons, and terminates with cyber-weapons (designed to attack computers or critical infrastructure) at the far end. As one moves along this continuum through the different so-called weapons of mass destruction (to which "cyber-weapons" have been added here for purposes of illustration), the difficulties facing nonproliferation become increasingly apparent. At the nuclear extreme, nonproliferation is comparatively robust, whereas at the cyber end it is enormously difficult.

Nuclear nonproliferation policy seeks to limit the number of nations that have nuclear weapons and keep such weapons out of the hands of subnational groups altogether. Any effective approach must guarantee warhead security and prevent the diversion of nuclear material from civilian programs to military or terrorist uses. Article III of the nuclear

Nonproliferation Treaty (NPT) provides the legal basis for a near-global verification regime to detect the diversion of fissile material—verification carried out by the UN's International Atomic Energy Agency (IAEA). The agency uses inspections, audits of nuclear material and records, and surveillance cameras and instrumentation to monitor more than 1,000 facilities worldwide.

The IAEA's verification efforts have worked in part because the facilities needed to produce uranium or plutonium for weapons are big and hard to hide. Of course, inspections are not foolproof. Iraq, for example, made significant progress in enrichment of indigenous uranium despite being a party to the NPT and subject to IAEA inspections. This experience led the IAEA to propose strengthened safeguards to include the right to inspections on short notice of undeclared, suspect locations. Yet there have also been important successes. In 1992, IAEA inspectors in North Korea found discrepancies indicating that a plutonium reprocessing plant at Yongbyon had been used more often than the government had declared. In the face of new challenges, the NPT verification regime must evolve rapidly enough to continue playing an important nonproliferation role.

The United States and the nearly 40 other nations of the Nuclear Suppliers Group further pursue nonproliferation by adhering to consensual guidelines restricting nuclear and nuclear-related "dual-use" exports—i.e., material that can serve both civilian and military purposes. These guidelines are intended to supplement the NPT by controlling the transfer of listed items without hindering the legitimate international nuclear cooperation called for by Article IV of the NPT. Through the Cooperative Threat Reduction (CTR) program with the Soviet Union's successor states, the United States has also acted to impede the theft or sale of nuclear material as well as the movement of nuclear scientists from the former Soviet Union to what the Clinton administration first called "rogue states" and later termed "states of concern." Of course, in addition to these multilateral and bilateral measures, diplomatic pressure and security guarantees have also played their roles, and intelligence has been vital throughout.

For all its difficulties, nuclear nonproliferation has been reasonably successful in part because the production of weapons-grade plutonium or uranium is difficult (requiring reactors or enrichment plants,

AP/WIDE WORLD PHOTOS

Cleaning House (and Senate): U.S. marines demonstrate anthrax removal, Capitol Hill, Washington, D.C., October 30, 2001

respectively), and this imposes conspicuous bottlenecks on any would-be weapons program. Few of the necessary facilities exist and they can be monitored if declared, or risk discovery by intelligence-gathering if not. (Of course, intelligence findings do not guarantee an end to proliferation concerns, as Iran's case shows.) Because the theft of weapons-grade nuclear material can allow a state or group to circumvent these bottlenecks, preventing nuclear theft has become a high priority in the post–Cold War world.

As challenging as preventing the spread of nuclear weapons has been, preventing the proliferation of cyber-weapons could be insurmountably difficult. Governments can and should control the export of certain high-end computers and components. But cyber-attacks can be launched from almost any of the more than 100 million computers worldwide that have access to the Internet. Applying standard nonproliferation techniques to these computers would therefore ultimately require unannounced inspections or the monitoring of hundreds of millions of residences and businesses. Cyber-security may benefit from certain nonproliferation measures, but it renders

traditional inspection approaches absurd. Moreover, automated monitoring of the source and content of electronic messages to identify illicit activities would face its own enormous obstacles.

Falling between the nuclear and cyber extremes of the WMD continuum are chemical, radiological, and biological weapons. Maintaining an international verification regime for chemical weapons is harder than for nuclear weapons because of the larger number of relevant facilities and dual-use materials. The Organization for the Prohibition of Chemical Weapons, established under the Chemical Weapons Convention (CWC), must contend with an entire industrial sector and more than 6,000 inspectable facilities. Nevertheless, under the CWC, governments have declared chemical weapons stocks and opened them to international verification, three of the four declared possessor states have begun destroying their stocks, and inspectors have examined hundreds of dual-use chemical plants. The declaration of 70,000 metric tons of chemical agents by the United States, Russia, India, and South Korea, along with additional states' declarations of chemical weapons production facilities, old chemical weapons, and abandoned chemical weapons, constitute a valuable achievement. The verified elimination of chemical stockpiles and the destruction or conversion of production facilities will be a clear gain for international security—especially once Russia begins destroying its 40,000 metric tons of chemical weapons, some of which currently remains vulnerable to theft. These achievements are valuable regardless of the disturbing absence of Iraq, North Korea, and other states of concern from the CWC regime. The regime is further supplemented by the Australia Group of 33 nations that, like the Nuclear Suppliers Group, establishes consensual national guidelines restricting the export of chemicals and technology that can be used to make weapons.

Biological weapons also fall between the nuclear and cyber ends of the WMD continuum but are even harder to control than chemical weapons. True, the Biological and Toxin Weapons Convention (BWC) established a norm against the production and stockpiling of biological weapons, and the 1925 Geneva Protocol forbids their use. The Australia Group also works to impede the transfer of biological agents and technology where possible through national export controls. Nevertheless, any biological nonproliferation regime will necessarily be less robust than its nuclear counterpart, because much of the relevant material, technology, and

knowledge is already far more widely distributed and will become more so in the coming decades.

Scientists can acquire potentially deadly biological agents in the course of legitimate research: for instance, U.S. and British government institutes previously distributed the Ames anthrax strain used in the autumn 2001 attacks to a dozen or so laboratories. Naturally occurring disease outbreaks are another source of lethal organisms: the Ames strain is common in eastern Texas, for example. Indeed, natural outbreaks are the ultimate origin of the agents historically used in nations' biological weapons programs. Moreover, the fermenters required to produce these biological agents in large quantities are widely used in the pharmaceutical, biotechnology, and even beer industries.

Weaponizing these diseases—going from the organism to a preparation that is particularly suitable for distribution as a powder or liquid aerosol—has proved difficult for terrorists. The Japanese group Aum Shinrikyo failed to weaponize anthrax despite devoting substantial financial and scientific resources to the task. But the group's repeated, unsuccessful attempts to spray liquid anthrax aerosol throughout downtown Tokyo in 1993 demonstrated that attacks designed to cause massive urban casualties were no longer in the realm of the fantastic. Then, last autumn's attacks in the United States, when professional-grade anthrax powder was sent through the mail, made clear that an individual or group has now either successfully crossed the weaponization threshold or succeeded in acquiring such material from a national weapons program.

Genetic modification of biological agents (to make them resistant to vaccines or antimicrobial drugs, for instance) probably remains beyond the capabilities of terrorist groups for the time being—although the illicit Soviet program did carry out such work and scientists have in effect done the same in research contexts. This sort of biotechnical know-how is spreading quickly.

BLOCKING BIOLOGY

THE CHALLENGES posed by biological nonproliferation—the dual-use character of materials and equipment, the small amounts of agents initially needed and their availability from natural outbreaks, and the dynamic nature of biotechnology—guarantee that an effective strategy

for biological security will look very different from the corresponding techniques used to curtail the spread of nuclear or chemical weapons. Biological security requires a different mix of nonproliferation, deterrence, and defense.

The BWC provides the legal basis for preventing the spread of biological weapons. However, the Bush administration in July 2001 rejected the draft compliance protocol to the BWC, arguing that it could jeopardize U.S. companies' proprietary information, did not provide sufficient protection for U.S. biodefense programs, and would not improve verification capabilities. By thus abandoning six years of negotiations, the United States is now not in a strong political position to pursue multilateral nonproliferation initiatives. Nevertheless, Washington should act to improve international control of dangerous pathogens, either within the BWC framework (perhaps by supporting the proposal of a like-minded ally) or in a new forum. Within the United States, the shipment of deadly diseases has been monitored since 1997. A national inventory and consolidation of facilities with dangerous strains and development of a gene library are the obvious next steps. Had these been in place in October 2001, the anthrax investigation could have proceeded more quickly.

Biological weapons are simply harder to control than nuclear or chemical ones.

Hundreds of culture collections containing dangerous organisms also exist around the world. Although terrorists can acquire pathogens from natural disease outbreaks, existing collections offer the easiest sources. The United States should therefore work with other nations to put into place international standards for the secure storage and transport of biological stocks that could be used for weapons. If it is no longer politically feasible for the United States to pursue such an objective within the BWC framework after having rejected the draft compliance protocol, it should consider, as Michael Barletta, Amy Sands, and Jonathan Tucker of the Monterey Institute of International Studies have suggested, pursuing a "Biosecurity Convention" to this end, consistent with, but if need be outside of, the BWC.

Certain bilateral steps are also crucial. The CTR and related programs have helped prevent the loss of biological-weapons scientists to states of

concern and provided the United States with details of the biological weapons programs in Ukraine, Kazakhstan, and Uzbekistan, as well as Russia's Biopreparat program. But other key Russian facilities under the ministries of defense and health have remained closed to outsiders. Spending for the biological component of CTR has now been increased from three percent to ten percent of the total CTR budget; at a minimum Washington should maintain this level of commitment. The Bush administration should also approach the Russian government at a high level so that the United States can inventory, consolidate, secure, and ultimately acquire samples or gene sequences of Russian bioweapons strains and conduct scientific exchanges with those Russian bioweapons facilities that remain closed. A similar bilateral agreement with Uzbekistan in summer 2001 gave the United States access to Vozrozhdeniye Island in the Aral Sea, where Americans will help dismantle Soviet-era bioweapons facilities and clean up remaining live agents, including those that resulted from open-air testing.

UNSTOPPABLE?

DETERRENCE through the threat of retaliation has been the central strategy for preventing the use of weapons of mass destruction against the United States or its allies. And deterrence may remain effective against a state's use of biological weapons. But biological terrorism by subnational groups poses special challenges in this regard. Deterring any form of terrorism is difficult, since some terrorist groups may be unconcerned about retaliation or may hope to remain unidentified. But the biological case is especially problematic. Because some diseases incubate without symptoms for days or even weeks, tracing an attack back to its perpetrators can prove difficult. Terrorists might even hope that their attack would go unrecognized as such. For instance, when followers of the Bhagwan Shree Rajneesh infected 750 Oregonians with salmonella in 1984, it was more than a year before authorities determined that the infection had been intentionally spread.

The summer 1999 outbreak of the West Nile virus in New York illustrates how difficult it can be in some circumstances to distinguish an intentional attack from a natural outbreak. Before the disease killed seven people in the New York City area, West Nile had never

before occurred in the western hemisphere. Due to bird migration, the virus has now spread to 27 states. Although the outbreak was apparently "natural" in origin, perhaps caused by an infected traveler or mosquito transported from the Middle East, it is remarkable that in April 1999, only a few months before the outbreak, an Iraqi defector had claimed that Saddam Hussein planned to weaponize the virus.

The United States should do what it can to increase the likelihood that an attack will be attributable. An essential resource is a DNA library of as many strains of relevant biological agents as can be assembled. DNA "fingerprinting" of the agent causing an outbreak is an important forensic tool, but it is most useful if the fingerprints are already on file. (DNA fingerprinting does not identify the perpetrator, however—only the weapon used. In this sense it is more like ballistics testing than human fingerprinting.) The United States needs a DNA library not only of natural and weaponized strains within U.S. collections but also of those located in inventories around the world. Again, cooperation with the states of the former Soviet Union is important.

In addition to the difficulties of attribution, some terrorist groups may also believe themselves to be invulnerable to retaliation, may be unconcerned by it, or may even intend to provoke it. Such groups are obviously poor candidates for deterrence through the threat of retaliation. However, deterrence by denial—deterring enemies by convincing them that biological defenses are credible and that therefore an attack would be unlikely to succeed—may be a more useful tool for biological security than it was for nuclear weapons. Of course, warning and prevention are preferable to coping with the consequences of an attack, so intelligence remains vital. But as the anthrax mail attacks made clear, biological terrorism can occur with little or no warning.

DEFENSE WITHOUT BORDERS

THE INTRINSIC CHALLENGES of stopping the spread of biological weapons, and the difficulties posed for deterrence suggest that biological security strategy should lean more heavily toward defense than has been true of nuclear or chemical security strategy. Building biological defenses will of course require appropriate steps by the Defense and Justice Departments. But just as important, and for too

long overlooked, biological security means improvements in domestic and international public health.

Prior to September 11, 2001, a number of analysts had in fact argued just this point: that a robust defense against bioterrorism must be based on improved public health. Because disease incubation times for some agents can be as long as weeks, the first responders to a biological attack are likely to be health care workers rather than fire, police, or military personnel. Public health surveillance for signs of unusual disease is therefore critical. Improvements in "sensitivity" and "connectivity" are required. Sensitivity means the recognition by health care workers that an illness is out of the ordinary; connectivity is the reporting of this recognition to local, state, and national authorities, and consequent timely help with diagnosis and treatment. The anthrax mail attacks tragically confirmed the importance of disease surveillance, since the speed with which doctors recognized the signs of anthrax infection determined whether patients were treated immediately or sent home, only to return later to die.

Biological security requires improvements in domestic and international public health.

In 1999, the U.S. government initiated the Biological Preparedness and Response Program (BPRP) within the Centers for Disease Control and Prevention. This program put in place many of the crucial steps required for a domestic public health defense against bioterrorism. The BPRP created the National Pharmaceutical Stockpile (NPS) of antibiotics and other drugs that could be rapidly deployed to counter domestic outbreaks. The BPRP also funded pilot projects to bolster disease surveillance, improved capacity at the state and local levels, and sponsored research. In fiscal year 2000, the BPRP budget stood at $155 million, an amount that some experts viewed as only one-tenth the funding needed for the tasks required. But at the time, there was legitimate disagreement—indeed, there still is—over the right balance between spending to prepare for rare but potentially disastrous events such as bioterrorism, and spending to counter naturally occurring infectious diseases that are already killing many individuals every day.

Nonetheless, the October 2001 anthrax crisis would have seemed far more dire had the NPS not existed, and the understandable public

tendency to begin self-medicating with antibiotics would have been even more difficult to contain. One of the great hazards of this response is its likely acceleration of antibiotic resistance in bacteria—resistance that can then be swapped between bacteria of different species. For the same reason, it is important that the poultry industry is reducing the quantities of antibiotics fed to healthy chickens, and analogous practices in other livestock industries should be similarly scrutinized. An effective biological security strategy must cast its net far wider than traditional national security issues.

Fortunately, many of the steps that are needed to prepare for bioterrorism will also improve recognition of and responses to natural disease outbreaks. Spending on biological defenses therefore represents a win-win situation in which society benefits even if no further bioterrorist attacks take place. The West Nile outbreak again provides an example: had better communication between veterinarians and public health officials existed in early summer 1999, when crows began to die in New York City, the outbreak could have been recognized months earlier.

After the anthrax mail attacks, attitudes toward domestic public health spending to prepare for bioterrorism rapidly changed. In a discussion of how much annual spending would be required to improve preparedness, a member of Congress remarked last autumn, "One or two billion dollars? That kind of money is easier done than said right now." Indeed, the 2002 emergency supplemental appropriations bill and a separate bioterrorism bill include billions of dollars in new spending for biological defense. These bills include steps to expand the pharmaceutical stockpile, increase stores of the smallpox vaccine, strengthen state and local preparedness, and improve food safety. Domestically, the right steps are being funded. The challenge will be to sustain this commitment as the psychological distance from September 11 grows.

Admittedly, not all measures taken against bioterrorism have dual uses. The NPS antibiotic supply is unlikely to be needed to counter natural outbreaks, and storing the smallpox vaccine prepares for a disease that no longer exists in the natural world. Because antibiotics have a finite shelf life, making the expanded NPS financially sustainable may require the government to create incentives for research into extending antibiotic shelf life (something that market forces themselves may not encourage) and ensuring sufficient extra production capacity in the event of a crisis.

Other forms of research must also continue. Standard antibiotics are effective against all the bacteria that are commonly listed as biological agents, but the Soviet bioweapons program produced strains of anthrax resistant to some antibiotics, and such bioengineering will become more widely available. Vaccines are available for some viral agents, such as smallpox, but there are no effective drugs for others, such as many of the viral hemorrhagic fevers (e.g., Ebola or Marburg, which the Soviets reportedly weaponized). For the foreseeable future, therefore, we are locked into a kind of biological defensive arms race in which researchers will need to develop different or more broadly effective antimicrobial drugs and vaccines against possible new threats.

An effective defense against bioterror also requires the means to distribute vaccines and antimicrobial drugs effectively, perhaps amid the extremely challenging circumstances of public panic. The effects of public fear should not be underestimated, and the lessons from real or potential mass casualty situations involving invisible, lingering threats are sobering. Aum Shinrikyo's 1995 sarin nerve gas attack in the Tokyo subway system injured hundreds of Japanese citizens, but 5,000 sought help at hospital emergency rooms. Similarly, when the governor of Pennsylvania in 1979 suggested the evacuation of pregnant women and preschool children living within a five-mile radius of the Three Mile Island nuclear power plant—in effect recommending that a few thousand people leave the area—between one and two hundred thousand fled. Responses to these sorts of reactions should be planned before crises occur.

BEYOND THE WATER'S EDGE

THE U.S. GOVERNMENT'S RESPONSE to last fall's bioterrorist attacks rightly highlighted the importance of domestic public health measures but showed little appreciation for the fact that no response can succeed if it stops at the nation's borders. International measures are crucial to a successful strategy for reasons as simple as arithmetic. Many diseases, such as plague and smallpox, have lengthy incubation times (an average of 2 to 3 days and 12 days, respectively). But the flight time between virtually any two cities in the world is now less than 36 hours. Carriers of smallpox, whether terrorists or unwitting victims, could transport the disease around the world before they ever showed signs

of illness. Some 140 million people enter the United States by air every year. Although improvements to border protection are important, neither the United States nor other nations can hope to protect themselves exclusively by guarding their frontiers. For both humanitarian and national security reasons, outbreaks of emerging infectious diseases need to be addressed overseas as well as domestically. When possible they should be prevented, but if that does not happen, such outbreaks need to be detected, diagnosed, and controlled as quickly as possible.

Any outbreak of a highly contagious, lethal, and long-incubating disease such as smallpox poses a grave international threat. In 1972, a single religious pilgrim returned to Yugoslavia from Mecca via several days in Iraq, where he had contracted smallpox. Smallpox had spread to Iraq from Iran, where a family had introduced it after acquiring it while traveling through Afghanistan. The disease in Yugoslavia went undiagnosed while the original infected individual spread the disease to others, one of whom traveled 100 miles by bus. To contain the resulting outbreak, Tito's government vaccinated 18 million people and quarantined some 10,000 in commandeered hotels and apartment buildings ringed with troops and barbed wire. By comparison, on September 11, 2001, the United States had fewer than 15 million doses of smallpox vaccine available to a larger and far more mobile society. Epidemiological models indicate that quarantine can to some extent be traded off against vaccination to control an outbreak. But better preparation with appropriate vaccines or drugs will diminish the curtailment of civil liberties that would otherwise be needed to control contagious outbreaks.

These lessons are not limited to bioterrorist outbreaks. AIDS is a naturally occurring disease that recently emerged in the human population. It has since killed more than 450,000 Americans and 22 million people worldwide. The importance of recognizing such new contagious illnesses early, rather than after they have spread across the globe, is terribly clear. The United States must act to prevent disease outbreaks, detect those (whether natural, artificial, or ambiguous) that do occur, and ensure an effective response. The six laboratories that the Defense Department has overseas to perform research on infectious diseases are an important resource that should be further strengthened, but a broader international response is also required.

Rapid detection of outbreaks requires improvements in international disease surveillance, for which the chronically underfunded World Health Organization (WHO) is central. In the event of a bioweapons attack abroad, reference laboratories (designed to examine environmental and medical samples) must be available overseas, or else U.S. domestic capacity will be swamped with international samples. Cost estimates begin in the tens of millions of dollars annually for minimal improvements in international disease surveillance and reference lab capacity, through the creation of regional WHO centers that build wherever possible on existing facilities. With its vast new spending on bioterrorism defense, the United States should allocate resources to fund these and other such serious, sustainable improvements in global public health. Whether the next threat is smallpox or a new AIDS-like epidemic disease, improving global infectious disease surveillance and response will be good for both humanitarian reasons and national security.

The United States is also creating a smallpox vaccine stockpile sufficient for all Americans. Although one recent epidemiological simulation suggests that a stockpile of 40 million doses would be sufficient to control likely outbreaks, it is difficult to predict whether a real attack would be as limited as that simulation assumes. Moreover, it should be clear from the public response to last autumn's anthrax scare that no White House will want to find itself in a position of having to explain to the American people why only some are eligible to receive vaccinations after an attack. The American people—like most people throughout the world—have for decades not been routinely vaccinated against smallpox, and the vaccine's effectiveness attenuates after ten years. The global population is now more vulnerable to smallpox than any large population has been since the illness devastated Native Americans after European explorers brought it to the Americas.

But even a stockpile for all U.S. citizens is insufficient. In the event of a smallpox outbreak overseas—whether in a NATO ally or in the developing world—humanitarian concern, international opinion, and its own self-interest will pressure the United States to shut down the outbreak and limit its spread. The WHO smallpox vaccine stockpile stands at half a million doses. The United States must either augment its national stockpile so that it can respond internationally without jeopardizing its own citizens or work with the WHO to increase international supplies. Of

course, the United States should encourage other nations to do the same, but it should not allow others' inaction to prevent it from acting in its own security interest to improve global public health.

SPEAKING TRUTH IN POWER

An effective strategy for biological security will encompass nonproliferation, deterrence, and defense, but the required mix of these components will be very different from those in strategies for nuclear or even chemical weapons. Perhaps most strikingly, effective biological security demands that the United States act to improve global disease surveillance and response capacity—an element of "defense" that has no good nuclear or chemical analogue. Biological security also requires ongoing research to counter emerging potential threats driven by biotechnology. It is as much about public health, science, and technology as it is about military strategy.

These needs emphasize the vital role that scientific advice will continue to play in national security. Yet the U.S. government is not well equipped to harness such advice. Congress eliminated its Office of Technology Assessment in 1995, and the president's science adviser has played a diminishing White House role over the past few decades. The Office of Science and Technology Policy, which is directed by the science adviser, is inherently weak bureaucratically. Few national security decisions naturally flow through it. As a result, the OSTP is only as strong in this arena as is the relationship between the science adviser and the president.

And too often, that relationship is weak. Both sides are to blame: too few scientists are good communicators and effective bureaucrats, and too few presidents recognize science as a priority. Nor does every policymaker appreciate that scientific integrity will at times require an unpopular answer. But as with intelligence, bending technical analysis to a particular policy risks producing deception rather than information.

The scientific and technical challenges of the coming decades will grow only more grave and incessant. Scientific complexity will be increasingly important for policymakers to understand and to communicate competently to the public. Policymakers must better incorporate scientific advice into their decision-making, or they risk falling prey to more, and more dangerous, misplaced analogies.