Towards a Chemical War in Syria ?

CBRNE Newsletter Terrorism

Volume 46, 2012

Bio News

www.cbrne-terrorism-newsletter.com

Hacking the President's DNA

By Andrew Hessel, Marc Goodman and Steven Kotler

Source:http://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/?single_page=true

The U.S. government is surreptitiously collecting the DNA of world leaders, and is reportedly protecting that of Barack Obama. Decoded, these genetic blueprints could provide compromising information. In the not-too-distant future, they may provide something more as well—the basis for the creation of personalized bioweapons that could take down a president and leave no trace.

This is how the future arrived. It began innocuously, in the early 2000s, when businesses started to realize that highly skilled jobs formerly performed in-house, by a single employee, could more efficiently be crowd-sourced to a larger group of people via the Internet. Initially, we crowd-sourced the design of T-shirts (Threadless.com) and the writing of encyclopedias (Wikipedia.com), but before long the trend started making inroads into the harder sciences. Pretty soon, the hunt for extraterrestrial life, the development of self-driving cars, and the folding of enzymes into novel proteins were being done this way. With the fundamental tools of genetic manipulation—tools that had cost millions of dollars not 10 years earlier—dropping precipitously in price, the crowd-sourced design of biological agents was just the next logical step.

In 2008, casual DNA-design competitions with small prizes arose; then in 2011, with the launch of GE's $100 million breast-cancer challenge, the field moved on to serious contests. By early 2015, as personalized gene therapies for end-stage cancer became medicine's cutting edge, virus-design Web sites began appearing, where people could upload information about their disease and virologists could post designs for a customized cure. Medically speaking, it all made perfect sense: Nature had done eons of excellent design work on viruses. With some retooling, they were ideal vehicles for gene delivery.

Soon enough, these sites were flooded with requests that went far beyond cancer. Diagnostic agents, vaccines, antimicrobials, even designer psychoactive drugs—all appeared on the menu. What people did with these bio-designs was anybody's guess. No international body had yet been created to watch over them.

So, in November of 2016, when a first-time visitor with the handle Cap'n Capsid posted a challenge on the viral-design site 99Virions, no alarms

sounded; his was just one of the 100 or so design requests submitted that day. Cap'n Capsid might have been some consultant to the pharmaceutical industry, and his challenge just another attempt to understand the radically shifting R&D landscape—really, he could have been anyone—but the problem was interesting nonetheless. Plus, Capsid was offering $500 for the winning design, not a bad sum for a few hours' work.

Later, 99Virions' log files would show that Cap'n Capsid's IP address originated in Panama, although this was likely a fake. The design specification itself raised no red flags. Written in SBOL, an open-source language popular with the synthetic-biology crowd, it seemed like a standard vaccine request. So people just got to work, as did the automated computer programs that had been written to "auto-evolve" new designs. These algorithms were getting quite good, now winning nearly a third of the challenges.

Within 12 hours, 243 designs were submitted, most by these computerized expert systems. But this time the winner, GeneGenie27, was actually human—a 20-year-old Columbia University undergrad with a knack for virology. His design was quickly forwarded to a thriving Shanghai-based online bio-marketplace. Less than a minute later, an Icelandic synthesis start-up won the contract to turn the 5,984-base-pair blueprint into actual genetic material. Three days after that, a package of 10-milligram, fast-dissolving microtablets was dropped in a FedEx envelope and handed to a courier.

Two days later, Samantha, a sophomore majoring in government at Harvard University, received the package. Thinking it contained a new synthetic psychedelic she had ordered online, she slipped a tablet into her left nostril that evening, then walked over to her closet. By the time Samantha finished dressing, the tab had started to dissolve, and a few strands of foreign genetic material had entered the cells of her nasal mucosa.

Some party drug—all she got, it seemed, was the flu. Later that night, Samantha had a slight fever and was shedding billions of virus particles. These particles would spread around campus in an exponentially growing chain reaction that was—other than the mild fever and some sneezing—absolutely harmless. This would change when the virus crossed paths with cells containing a very specific DNA sequence, a sequence that would act as a molecular key to unlock secondary functions that were not so benign. This secondary sequence would trigger a fast-acting neuro-destructive disease that produced memory loss and, eventually, death. The only person in the world with this DNA sequence was the president of the United States, who was scheduled to speak at Harvard's Kennedy School of Government later that week. Sure, thousands of people on campus would be sniffling, but the Secret Service probably wouldn't think anything was amiss.

It was December, after all—cold-and-flu season.

The scenario we've just sketched may sound like nothing but science fiction—and, indeed, it does contain a few futuristic leaps. Many members of the scientific community would say our time line is too fast. But consider that since the beginning of this century, rapidly accelerating technology has shown a distinct tendency to turn the impossible into the everyday in no time at all. Last year, IBM's Watson, an artificial intelligence, understood natural language well enough to whip the human champion Ken Jennings on *Jeopardy*. As we write this, soldiers with bionic limbs are returning to active duty, and autonomous cars are driving down our streets. Yet most of these advances are small in comparison with the great leap forward currently under way in the biosciences—a leap with consequences we've only begun to imagine.

More to the point, consider that the DNA of world leaders is already a subject of intrigue. According to Ronald Kessler, the author of the 2009 book *In the President's Secret Service*, Navy stewards gather bedsheets, drinking glasses, and other objects the president has touched—they are later sanitized or destroyed—in an effort to keep would-be malefactors from obtaining his genetic material. (The Secret Service would neither confirm nor deny this practice, nor would it comment on any other aspect of this article.) And according to a 2010 release of secret cables by WikiLeaks, Secretary of State Hillary Clinton directed our embassies to surreptitiously collect DNA samples from foreign heads of state and senior United Nations officials. Clearly, the U.S. sees strategic advantage in knowing the specific biology of world leaders; it would be surprising if other nations didn't feel the same.

While no use of an advanced, genetically targeted bio-weapon has been reported, the authors of this piece—including an expert in genetics and microbiology (Andrew Hessel) and one in global security and law enforcement (Marc Goodman)—are convinced we are drawing close to this possibility. Most of the enabling technologies are in place, already serving the needs of academic R&D groups and commercial biotech organizations. And these technologies are becoming exponentially more powerful, particularly those that allow for the easy manipulation of DNA.

The evolution of cancer treatment provides one window into what's happening. Most cancer drugs kill cells. Today's chemotherapies are offshoots of chemical-warfare agents: we've turned weapons into cancer medicines, albeit crude ones—and as with carpet bombing, collateral damage is a given. But now, thanks to advances in genetics, we know that each cancer is unique, and research is shifting to the development of personalized medicines—designer therapies that can exterminate specific cancerous cells in a specific way, in a specific person; therapies focused like lasers.

To be sure, around the turn of the millennium, significant fanfare surrounded personalized medicine, especially in the field of genetics. A lot of that is now gone. The prevailing wisdom is that the tech has not lived up to the talk, but this isn't surprising. Gartner, an information-technology research-and-advisory firm, has coined the term *hype cycle* to describe exactly this sort of phenomenon: a new technology is introduced with enthusiasm, only to be followed by an emotional low when it fails to immediately deliver on its promise. But Gartner also discovered that the cycle doesn't typically end in what the firm calls "the trough of disillusionment." Rising from those ashes is a "slope of enlightenment"—meaning that when viewed from a longer-term historical perspective, the majority of these much-hyped groundbreaking developments do, eventually, break plenty of new ground.

As George Church, a geneticist at Harvard, explains, this is what is now happening in personalized medicine. "The fields of gene therapies, viral delivery, and other personalized therapies are progressing rapidly," Church says, "with several clinical trials succeeding into Phase 2 and 3," when the therapies are tried on progressively larger numbers of test subjects. "Many of these treatments target cells that differ in only one—rare—genetic variation relative to surrounding cells or individuals." The Finnish start-up Oncos Therapeutics has already treated close to 300 cancer patients using a scaled-down form of this kind of targeted technology.

These developments are, for the most part, positive—promising better treatment, new cures, and, eventually, longer life. But it wouldn't take much to subvert such therapies and come full circle, turning personalized medicines into personalized bioweapons. "Right now," says Jimmy Lin, a genomics researcher at Washington University in St. Louis and the founder of Rare Genomics, a nonprofit organization that designs treatments for rare childhood diseases based on individual genetic analysis, "we have drugs that target specific cancer mutations. Examples include Gleevec, Zelboraf, and Xalkori. Vertex," a pharmaceutical company based in Massachusetts, "has famously made a drug for cystic-fibrosis patients with a particular mutation. The genetic targeting of individuals is a little farther out. But a state-sponsored program of the Stuxnet variety might be able to accomplish this in a few years. Of course, this work isn't very well known, so if you tell most people about this, they say that the time frame sounds like science fiction. But when you're familiar with the research, it's really feasible that a well-funded group could pull this off." We would do well to begin planning for that possibility sooner rather than later.

If you really want to understand what's happening in the biosciences, then you need to understand the rate at which information technology is accelerating. In 1965, Gordon Moore famously realized that the number of integrated-circuit components on a computer chip had been doubling roughly every year since the invention of the integrated circuit in the late 1950s. Moore, who would go on to co-found Intel, predicted that the trend would continue "for at least 10 years." He was right. The trend did continue for 10 years, and 10 more after that. All told, his observation has remained accurate for five decades, becoming so durable that it's now known as "Moore's Law" and used by the semi-conductor industry as a guide for future planning.

Moore's Law originally stated that every 12 months (it is now 24 months), the number of transistors on an integrated circuit will double—an

example of a pattern known as "exponential growth." While linear growth is a slow, sequential proposition (1 becomes 2 becomes 3 becomes 4, etc.), exponential growth is an explosive doubling (1 becomes 2 becomes 4 becomes 8, etc.) with a transformational effect. In the 1970s, the most powerful supercomputer in the world was a Cray. It required a small room to hold it and cost roughly $8 million. Today, the iPhone in your pocket is more than 100 times faster and more than 12,000 times cheaper than a Cray. This is exponential growth at work.

In the years since Moore's observation, scientists have discovered that the pattern of exponential growth occurs in many other industries and technologies. The amount of Internet data traffic in a year, the number of bytes of computer data storage available per dollar, the number of digital-camera pixels per dollar, and the amount of data transferable over optical fiber are among the dozens of measures of technological progress that follow this pattern. In fact, so prevalent is exponential growth that researchers now suspect it is found in all information-based technology—that is, any technology used to input, store, process, retrieve, or transmit digital information.

Over the past few decades, scientists have also come to see that the four letters of the genetic alphabet—A (adenine), C (cytosine), G (guanine), and T (thymine)—can be transformed into the ones and zeroes of binary code, allowing for the easy, electronic manipulation of genetic information. With this development, biology has turned a corner, morphing into an information-based science and advancing exponentially. As a result, the fundamental tools of genetic engineering, tools designed for the manipulation of life—tools that could easily be co-opted for destructive purposes—are now radically falling in cost and rising in power. Today, anyone with a knack for science, a decent Internet connection, and enough cash to buy a used car has what it takes to try his hand at bio-hacking.

These developments greatly increase several dangers. The most nightmarish involve bad actors creating weapons of mass destruction, or careless scientists unleashing accidental plagues—very real concerns that urgently need more attention. Personalized bioweapons, the focus of this story, are a subtler and less catastrophic threat, and perhaps for that reason, society has barely begun to consider them. Yet once available, they will, we believe, be put into use much more readily than bioweapons of mass destruction. For starters, while most criminals might think twice about mass slaughter, murder is downright commonplace. In the future, politicians, celebrities, leaders of industry—just about anyone, really—could be vulnerable to attack-by-disease. Even if fatal, many such attacks could go undetected, mistaken for death by natural causes; many others would be difficult to pin on a suspect, especially given the passage of time between exposure and the appearance of symptoms.

Moreover—as we'll explore in greater detail—these same scientific developments will pave the way, eventually, for an entirely new kind of personal warfare. Imagine inducing extreme paranoia in the CEO of a large corporation so as to gain a business advantage, for example; or—further out in the future—infecting shoppers with the urge to impulse-buy.

We have chosen to focus this investigation mostly on the president's bio-security, because the president's personal welfare is paramount to national security—and because a discussion of the challenges faced by those charged with his protection will illuminate just how difficult (and different) "security" will be, as biotechnology continues to advance.

A direct assault against the president's genome requires first being able to decode genomes. Until recently, this was no simple matter. In 1990, when the U.S. Department of Energy and the National Institutes of Health announced their intention to sequence the 3 billion base pairs of the human genome over the next 15 years, it was considered the most ambitious life-sciences project ever undertaken. Despite a budget of $3 billion, progress did not come quickly. Even after years of hard work, many experts doubted that the time and money budgeted would be enough to complete the job.

This started to change in 1998, when the entrepreneurial biologist J. Craig Venter and his company, Celera, got into the race. Taking advantage of the exponential growth in biotechnology, Venter relied on a new generation of gene sequencers and a novel, computer-intensive approach called shotgun sequencing to deliver a draft human genome (his own) in less than two years, for $300 million.

Venter's achievement was stunning; it was also just the beginning. By 2007, just seven years later, a human genome could be sequenced for less than $1 million. In 2008, some labs would do it for $60,000, and in 2009, $5,000. This year, the $1,000 barrier looks likely to fall. At the current rate of decline, within five years, the cost will be less than $100. In the history of the world, perhaps no other technology has dropped in price and increased in performance so dramatically.

Still, it would take more than just a gene sequencer to build a personally targeted bioweapon. To begin with, prospective attackers would have to collect and grow live cells from the target (more on this later), so cell-culturing tools would be a necessity. Next, a molecular profile of the cells would need to be generated, involving gene sequencers, micro-array scanners, mass spectrometers, and more. Once a detailed genetic blueprint had been built, the attacker could begin to design, build, and test a pathogen, which starts with genetic databases and software and ends with virus and cell-culture work. Gathering the equipment required to do all of this isn't trivial, and yet, as researchers have upgraded to new tools, as large companies have merged and consolidated operations, and as smaller shops have run out of money and failed, plenty of used lab equipment has been dumped onto the resale market. New, the requisite gear would cost well over $1 million. On eBay, it can be had for as little as $10,000. Strip out the analysis equipment—since those processes can now be outsourced—and a basic cell-culture rig can be cobbled together for less than $1,000. Chemicals and lab supplies have never been easier to buy; hundreds of Web resellers take credit cards and ship almost anywhere.

Biological knowledge, too, is becoming increasingly democratized. Web sites like JoVE (*Journal of Visualized Experiments*) provide thousands of how-to videos on the techniques of bioscience. MIT offers online courses. Many journals are going open-access, making the latest research, complete with detailed sections on materials and methods, freely available. If you wanted a more hands-on approach to learning, you could just immerse yourself in any of the dozens of do-it-yourself-biology organizations, such as Genspace and BioCurious, that have lately sprung up to make genetic engineering into something of a hobbyist's pursuit. Bill Gates, in a recent interview, told a reporter that if he were a kid today, forget about hacking computers: he'd be hacking biology. And for those with neither the lab nor the learning, dozens of Contract Research and Manufacturing Services (known as CRAMS) are willing to do much of the serious science for a fee.

From the invention of genetic engineering in 1972 until very recently, the high cost of equipment, and the high cost of education to use that equipment effectively, kept most people with ill intentions away from these technologies. Those barriers to entry are now almost gone. "Unfortunately," Secretary Clinton said in a December 7, 2011, speech to the Biological and Toxin Weapons Convention Review Conference, "the ability of terrorists and other non-state actors to develop and use these weapons is growing. And therefore, this must be a renewed focus of our efforts … because there are warning signs, and they are too serious to ignore."

The radical expansion of biology's frontier raises an uncomfortable question: How do you guard against threats that don't yet exist? Genetic engineering sits at the edge of a new era. The old era belonged to DNA sequencing, which is simply the act of reading genetic code—identifying and extracting meaning from the ordering of the four chemicals that make up DNA. But now we're learning how to *write* DNA, and this creates possibilities both grand and terrifying.

Again, Craig Venter helped to usher in this shift. In the mid-1990s, just before he began his work to read the human genome, he began wondering what it would take to write one. He wanted to know what the minimal genome required for life looked like. It was a good question. Back then, DNA-synthesis technology was too crude and expensive for anyone to consider writing a minimal genome for life or, more to our point, constructing a sophisticated bioweapon. And gene-splicing techniques, which involve the tricky work of using enzymes to cut up existing DNA from one or more organisms and stitch it back together, were too unwieldy for the task.

Exponential advances in biotechnology have greatly diminished these problems. The latest technology—known as synthetic biology, or "synbio"—moves the work from the molecular to the digital. Genetic code is manipulated

using the equivalent of a word processor. With the press of a button, code representing DNA can be cut and pasted, effortlessly imported from one species into another. It can be reused and repurposed. DNA bases can be swapped in and out with precision. And once the code looks right? Simply hit Send. A dozen different DNA print shops can now turn these bits into biology.

In May 2010, with the help of these new tools, Venter answered his own question by creating the world's first synthetic self-replicating chromosome. To pull this off, he used a computer to design a novel bacterial genome (of more than 1 million base pairs in total). Once the design was complete, the code was e-mailed to Blue Heron Biotechnology, a Seattle-area company that specializes in synthesizing DNA from digital blueprints. Blue Heron took Venter's A's, T's, C's, and G's and returned multiple vials filled with frozen plasmid DNA. Just as one might load an operating system into a computer, Venter then inserted the synthetic DNA into a host bacterial cell that had been emptied of its own DNA. The cell soon began generating proteins, or, to use the computer term popular with today's biologists, it "booted up": it started to metabolize, grow, and, most important, divide, based entirely on the code of the injected DNA. One cell became two, two became four, four became eight. And each new cell carried only Venter's synthetic instructions. For all practical purposes, it was an altogether new life form, created virtually from scratch. Venter called it "the first self-replicating species that we've had on the planet whose parent is a computer."

But Venter merely grazed the surface. Plummeting costs and increasing technical simplicity are allowing synthetic biologists to tinker with life in ways never before feasible. In 2006, for example, Jay D. Keasling, a biochemical engineer at the University of California at Berkeley, stitched together 10 synthetic genes made from the genetic blueprints of three different organisms to create a novel yeast that can manufacture the precursor to the antimalarial drug artemisinin, artemisinic acid, natural supplies of which fluctuate greatly. Meanwhile, Venter's company Synthetic Genomics is working in partnership with ExxonMobil on a designer algae that consumes carbon dioxide and excretes biofuel; his spin-off company Synthetic Genomics Vaccines is trying to develop flu-fighting vaccines that can be made in hours or days instead of the six-plus months now required. Solazyme, a synbio company based in San Francisco, is making biodiesel with engineered micro-algae. Material scientists are also getting in on the action: DuPont and Tate & Lyle, for instance, have jointly designed a highly efficient and environmentally friendly organism that ingests corn sugar and excretes propanediol, a substance used in a wide range of consumer goods, from cosmetics to cleaning products.

Other synthetic biologists are playing with more-fundamental cellular mechanisms. The Florida-based Foundation for Applied Molecular Evolution has added two bases (Z and P) to DNA's traditional four, augmenting the old genetic alphabet. At Harvard, George Church has supercharged evolution with his Multiplex Automated Genome Engineering process, which randomly swaps multiple genes at once. Instead of creating novel genomes one at a time, MAGE creates billions of variants in a matter of days.

Finally, because synbio makes DNA design, synthesis, and assembly easier, we're already moving from the tweaking of existing genetic designs to the construction of new organisms—species that have never before been seen on Earth, species birthed entirely by our imagination. Since we can control the environments these organisms will live in—adjusting things like temperature, pressure, and food sources while eliminating competitors and other stresses—we could soon be generating creatures capable of feats impossible in the "natural" world. Imagine organisms that can thrive on the surface of Mars, or enzymes able to change simple carbon into diamonds or nanotubes. The ultimate limits to synthetic biology are hard to discern.

All of this means that our interactions with biology, already complicated, are about to get a lot more troublesome. Mixing together code from multiple species or creating novel organisms could have unintended consequences. And even in labs with high safety standards, accidents happen. If those accidents involve a containment breach, what is today a harmless laboratory bacterium could tomorrow become an ecological catastrophe. A 2010 synbio report by the Presidential Commission for the Study of Bioethical Issues said as

much: "Unmanaged release could, in theory, lead to undesired cross-breeding with other organisms, uncontrolled proliferation, crowding out of existing species, and threats to biodiversity."

Just as worrisome as bio-error is the threat of bioterror. Although the bacterium Venter created is essentially harmless to humans, the same techniques could be used to construct a known pathogenic virus or bacterium or, worse, to engineer a much deadlier version of one. Viruses are particularly easy to synthetically engineer, a fact made apparent in 2002, when Eckard Wimmer, a Stony Brook University virologist, chemically synthesized the polio genome using mail-order DNA. At the time, the 7,500-nucleotide synthesis cost about $300,000 and took several years to complete. Today, a similar synthesis would take just weeks and cost a few thousand dollars. By 2020, if trends continue, it will take a few minutes and cost roughly $3. Governments the world over have spent billions trying to eradicate polio; imagine the damage terrorists could do with a $3 pathogen.

During the 1990s, the Japanese cult Aum Shinrikyo, infamous for its deadly 1995 sarin-gas attack on the Tokyo subway system, maintained an active and extremely well-funded bioweapons program, which included anthrax in its arsenal. When police officers eventually raided its facilities, they found proof of a years-long research effort costing an estimated $30 million—demonstrating, among other things, that terrorists clearly see value in pursuing bioweaponry. Although Aum did manage to cause considerable harm, it failed in its attempts to unleash a bioweapon of mass destruction. In a 2001 article for *Studies in Conflict & Terrorism*, William Rosenau, a terrorism expert then at the Rand Corporation, explained:

Aum's failure suggests that it may, in fact, be far more difficult to carry out a deadly bioterrorism attack than has sometimes been portrayed by government officials and the press. Despite its significant financial resources, dedicated personnel, motivation, and freedom from the scrutiny of the Japanese authorities, Aum was unable to achieve its objectives.

That was then; this is now. Today, two trends are changing the game. The first began in 2004, when the International Genetically Engineered Machine (iGEM) competition was launched at MIT. In this competition, teams of high-school and college students build simple biological systems from standardized, interchangeable parts. These standardized parts, now known as BioBricks, are chunks of DNA code, with clearly defined structures and functions, that can be easily linked together in new combinations, a little like a set of genetic Lego bricks. iGEM collects these designs in the Registry of Standard Biological Parts, an open-source database of downloadable BioBricks accessible to anyone.

Over the years, iGEM teams have pushed not only technical barriers but creative ones as well. By 2008, students were designing organisms with real-world applications; the contest that year was won by a team from Slovenia for its designer vaccine against *Helicobacter pylori*, the bacterium responsible for most ulcers. The 2011 grand-prize winner, a team from the University of Washington, completed three separate projects, each one rivaling the outputs of world-class academics and the biopharmaceutical industry. Teams have turned bacterial cells into everything from photographic film to hemoglobin-producing blood substitutes to miniature hard drives, complete with data encryption.

As the sophistication of iGEM research has risen, so has the level of participation. In 2004, five teams submitted 50 potential BioBricks to the registry. Two years later, 32 teams submitted 724 parts. By 2010, iGEM had mushroomed to 130 teams submitting 1,863 parts—and the registry database was more than 5,000 components strong. As *The New York Times* pointed out:

iGEM has been grooming an entire generation of the world's brightest scientific minds to embrace synthetic biology's vision—without anyone really noticing, before the public debates and regulations that typically place checks on such risky and ethically controversial new technologies have even started.

(igem itself does require students to be mindful of any ethical or safety issues, and encourages public discourse on these questions.)

The second trend to consider is the progress that terrorist and criminal organizations have made with just about every other information technology. Since the birth of the digital revolution, some early adopters have turned out to be rogue actors. Phone phreakers like John Draper (aka "Captain Crunch") discovered back in

the 1970s that AT&T's telephone network could be fooled into allowing free calls with the help of a plastic whistle given away in cereal boxes (thus Draper's moniker). In the 1980s, early desktop computers were subverted by a sophisticated array of computer viruses for malicious fun—then, in the 1990s, for information theft and financial gain. The 2000s saw purportedly uncrackable credit-card cryptographic algorithms reverse-engineered and smartphones repeatedly infected with malware. On a larger scale, denial-of-service attacks have grown increasingly destructive, crippling everything from individual Web sites to massive financial networks. In 2000, "Mafiaboy," a Canadian high-school student acting alone, managed to freeze or slow down the Web sites of Yahoo, eBay, CNN, Amazon, and Dell.

In 2007, Russian hackers swamped Estonian Web sites, disrupting financial institutions, broadcasting networks, government ministries, and the Estonian parliament. A year later, the nation of Georgia, before the Russian invasion, saw a massive cyberattack paralyze its banking system and disrupt cellphone networks. Iraqi insurgents subsequently repurposed SkyGrabber—cheap Russian software frequently used to steal satellite television—to intercept the video feeds of U.S. Predator drones in order to monitor and evade American military operations.

Lately, organized crime has taken up crowd-sourcing parts of its illegal operations—printing up fake credit cards, money laundering—to people or groups with specialized skills. (In Japan, the *yakuza* has even begun to outsource murder, to Chinese gangs.) Given the anonymous nature of the online crowd, it is all but impossible for law enforcement to track these efforts.

The historical trend is clear: Whenever novel technologies enter the market, illegitimate uses quickly follow legitimate ones. A black market soon appears. Thus, just as criminals and terrorists have exploited many other forms of technology, they will surely soon turn to synthetic biology, the latest digital frontier.

In 2005, as part of its preparation for this threat, the FBI hired Edward You, a cancer researcher at Amgen and formerly a gene therapist at the University of Southern California's Keck School of Medicine. You, now a supervisory special agent in the Weapons of Mass Destruction Directorate within the FBI's Biological Countermeasures Unit, knew that biotechnology had been expanding too quickly for the bureau to keep pace, so he decided the only way to stay ahead of the curve was to develop partnerships with those at the leading edge. "When I got involved," You says, "it was pretty clear the FBI wasn't about to start playing Big Brother to the life sciences. It's not our mandate, and it's not possible. All the expertise lies in the scientific community. Our job has to be outreach education. We need to create a culture of security in the synbio community, of responsible science, so the researchers themselves understand that they are the guardians of the future."

Toward that end, the FBI started hosting free bio-security conferences, stationed WMD outreach coordinators in 56 field offices to network with the synbio community (among other responsibilities), and became an iGEM partner. In 2006, after reporters at *The Guardian* successfully mail-ordered a crippled fragment of the genome for the smallpox virus, suppliers of genetic materials decided to develop self-policing guidelines. According to You, the FBI sees the organic emergence of these guidelines as proof that its community-based policing approach is working. However, we are not so sure these new rules do much besides guarantee that a pathogen isn't sent to a P.O. box.

In any case, much more is necessary. An October 2011 report by the WMD Center, a nonprofit organization led by former Senators Bob Graham (a Democrat) and Jim Talent (a Republican), said a terrorist-sponsored WMD strike somewhere in the world was probable by the end of 2013—and that the weapon would most likely be biological. The report specifically highlighted the dangers of synthetic biology:

> *As DNA synthesis technology continues to advance at a rapid pace, it will soon become feasible to synthesize nearly any virus whose DNA sequence has been decoded ... as well as artificial microbes that do not exist in nature.*

This growing ability to engineer life at the molecular level carries with it the risk of facilitating the development of new and more deadly biological weapons.

Malevolent non-state actors are not the only danger to consider. Forty nations now host synbio research, China among them. The Beijing

Genomics Institute, founded in 1999, is the largest genomic-research organization in the world, sequencing the equivalent of roughly 700,000 human genomes a year. (In a recent *Science* article, BGI claimed to have more sequencing capacity than all U.S. labs combined.) Last year, during a German *E. coli* outbreak, when concerns were raised that the disease was a new, particularly deadly strain, BGI sequenced the culprit in just three days. To put that in perspective, SARS—the deadly pneumonia variant that panicked the world in 2003—was sequenced in 31 days. And BGI appears poised to move beyond DNA sequencing and become one of the foremost DNA synthesizers as well.

BGI hires thousands of bright young researchers each year. The training is great, but the wages are reportedly low. This means that many of its talented synthetic biologists may well be searching for better pay and greener pastures each year, too. Some of those jobs will undoubtedly appear in countries not yet on the synbio radar. Iran, North Korea, and Pakistan will almost certainly be hiring.

In the run-up to Barack Obama's inauguration, threats against the incoming president rose markedly. Each of those threats had to be thoroughly investigated. In his book on the Secret Service, Ronald Kessler writes that in January 2009, for example, when intelligence emerged that the Somalia-based Islamist group al-Shabaab might try to disrupt Obama's inauguration, the Secret Service's mandate for that day became even harder. In total, Kessler reports, the Service coordinated some 40,000 agents and officers from 94 police, military, and security agencies. Bomb-sniffing dogs were deployed throughout the area, and counter-sniper teams were stationed along the parade route. This is a considerable response capability, but in the future, it won't be enough. A complete defense against the weapons that synbio could make possible has yet to be invented.

The range of threats that the Secret Service has to guard against already extends far beyond firearms and explosive devices. Both chemical and radiological attacks have been launched against government officials in recent years. In 2004, the poisoning of the Ukrainian presidential candidate Viktor Yushchenko involved TCCD, an extremely toxic dioxin compound. Yushchenko survived, but was severely scarred by chemically induced lesions. In 2006, Alexander Litvinenko, a former officer of the Russian security service, was poisoned to death with the radioisotope polonium 210. And the use of bioweapons themselves is hardly unknown; the 2001 anthrax attacks in the United States nearly reached members of the Senate.

The Kremlin, of course, has been suspected of poisoning its enemies for decades, and anthrax has been around for a while. But genetic technologies open the door for a new threat, in which a head of state's own DNA could be used against him or her. This is particularly difficult to defend against. No amount of Secret Service vigilance can ever fully secure the president's DNA, because an entire genetic blueprint can now be produced from the information within just a single cell. Each of us sheds millions and millions of cells every day. These can be collected from any number of sources—a used tissue, a drinking glass, a toothbrush. Every time President Obama shakes hands with a constituent, Cabinet member, or foreign leader, he's leaving an exploitable genetic trail. Whenever he gives away a pen at a bill-signing ceremony, he gives away a few cells too. These cells are dead, but the DNA is intact, allowing for the revelation of potentially compromising details of the president's biology.

To build a bioweapon, living cells would be the true target (although dead cells may suffice as soon as a decade from now). These are more difficult to recover. A strand of hair, for example, is dead, but if that hair contains a follicle, it also contains living cells. A sample gathered from fresh blood or saliva, or even a sneeze, caught in a discarded tissue, could suffice. Once recovered, these living cells can be cultured, providing a continuous supply of research material.

Even if Secret Service agents were able to sweep up all the shed cells from the president's current environs, they couldn't stop the recovery of DNA from the president's past. DNA is a very stable molecule, and can last for millennia. Genetic material remains present on old clothes, high-school papers—any of the myriad objects handled and discarded long before the announcement of a presidential candidacy. How much attention was dedicated to protecting Barack Obama's DNA when he was a senator? A community organizer in Chicago? A student at Harvard Law?

A kindergartner? And even if presidential DNA were somehow fully locked down, a good approximation of the code could be made from cells of the president's children, parents, or siblings, living or not.

Presidential DNA could be used in a variety of politically sensitive ways, perhaps to fabricate evidence of an affair, fuel speculation about birthplace and heritage, or identify genetic markers for diseases that could cast doubt on leadership ability and mental acuity. How much would it take to unseat a president? The first signs of Ronald Reagan's Alzheimer's may have emerged during his second term. Some doctors today feel the disease was then either latent or too mild to affect his ability to govern. But if information about his condition had been genetically confirmed and made public, would the American people have demanded his resignation? Could Congress have been forced to impeach him?

For the Secret Service, these new vulnerabilities conjure attack scenarios worthy of a Hollywood thriller. Advances in stem-cell research make any living cell transformable into many other cell types, including neurons or heart cells or even in vitro–derived (IVD) "sperm." Any live cells recovered from a dirty glass or a crumpled napkin could, in theory, be used to manufacture synthetic sperm cells. And so, out of the blue, a president could be confronted by a "former lover" coming forward with DNA evidence of a sexual encounter, like a semen stain on a dress. Sophisticated testing could distinguish an IVD fake sperm from the real thing—they would not be identical—but the results might never be convincing to the lay public. IVD sperm may also someday prove capable of fertilizing eggs, allowing for "love children" to be born using standard in vitro fertilization.

In the hope of mounting the best defense, one option is radical transparency: release the president's DNA.

As mentioned, even modern cancer therapies could be harnessed for malicious ends. Personalized therapies designed to attack a specific patient's cancer cells are already moving into clinical trials. Synthetic biology is poised to expand and accelerate this process by making individualized viral therapies inexpensive. Such "magic bullets" can target cancer cells with precision. But what if these bullets were trained to attack healthy cells instead? Trained against retinal cells, they would produce blindness. Against the hippocampus, a memory wipe may result. And the liver? Death would follow in months.

The delivery of this sort of biological agent would be very difficult to detect. Viruses are tasteless and odorless and easily aerosolized. They could be hidden in a perfume bottle; a quick dab on the attacker's wrist in the general proximity of the target is all an assassination attempt would require. If the pathogen were designed to zero in specifically on the president's DNA, then nobody else would even fall ill. No one would suspect an attack until long after the infection.

Pernicious agents could be crafted to do their damage months or even years after exposure, depending on the goals of the designer. Several viruses are already known to spark cancers. New ones could eventually be designed to infect the brain with, for instance, synthetic schizophrenia, bipolar disorder, or Alzheimer's. Stranger possibilities exist as well. A disease engineered to amplify the production of cortisol and dopamine could induce extreme paranoia, turning, say, a peace-seeking dove into a warmongering hawk. Or a virus that boosts the production of oxytocin, the chemical likely responsible for feelings of trust, could play hell with a leader's negotiating abilities. Some of these ideas aren't new. As far back as 1994, the U.S. Air Force's Wright Laboratory theorized about chemical-based pheromone bombs.

Of course, heads of state would not be the only ones vulnerable to synbio threats. Al-Qaeda flew planes into buildings to cripple Wall Street, but imagine the damage an attack targeting the CEOs of a number of *Fortune* 500 companies could do to the world economy. Forget kidnapping rich foreign nationals for ransom; kidnapping their DNA might one day be enough. Celebrities will face a new kind of stalker. As home-brew biology matures, these technologies could end up being used to "settle" all sorts of disputes, even those of the domestic variety. Without question, we are near the dawn of a brave new world.

How might we protect the president in the years ahead, as biotech continues to advance? Despite the acceleration of readily exploitable biotechnology, the Secret Service is not powerless. Steps can be taken to limit risks. The agency would not reveal what defenses are already in place, but establishing a crack scientific task

force within the agency to monitor, forecast, and evaluate new biotechnological risks would be an obvious place to start. Deploying sensing technologies is another possibility. Already, bio-detectors have been built that can sense known pathogens in less than three minutes. These can get better—a *lot* better—but even so, they might be limited in their effectiveness. Because synbio opens the door to new, finely targeted pathogens, we'd need to detect that which we've never seen before. In this, however, the Secret Service has a big advantage over the Centers for Disease Control and Prevention or the World Health Organization: its principal responsibility is the protection of one *specific* person. Bio-sensing technologies could be developed around the president's actual genome. We could use his living cells to build an early-warning system with molecular accuracy.

Cultures of live cells taken from the president could also be kept at the ready—the biological equivalent to data backups. The Secret Service reportedly already carries several pints of blood of the president's type in his motorcade, in case an emergency transfusion becomes necessary. These biological backup systems could be expanded to include "clean DNA"—essentially, verified stem-cell libraries that would allow bone-marrow transplantation or the enhancement of antiviral or antimicrobial capabilities. As so-called tissue-printing technologies improve, the president's cells could even be turned, one day, into ready-made standby replacement organs.

Yet even if the Secret Service were to implement some or all of these measures, there is no guarantee that the presidential genome could be completely protected. Anyone truly determined to get the president's DNA would probably succeed, no matter the defenses. And the Secret Service might have to accept that it can't fully counter all bio-threats, any more than it can guarantee that the president will never catch a cold.

In the hope of mounting the best defense against an attack, one possible solution—not without its drawbacks—is radical transparency: release the president's DNA and other relevant biological data, either to a select group of security-cleared bioscience researchers or (the far more controversial step) to the public at large. These ideas may seem counterintuitive, but we have come to believe that open-sourcing this problem—and actively engaging the American public in the challenge of protecting its leader—might turn out to be the best defense.

One practical reason is cost. Any in-house protection effort would be exceptionally pricey. Certainly, considering what's at stake, the country would bear the expense, but is that the best solution? After all, over the past five years, DIY Drones, a nonprofit online community of autonomous aircraft hobbyists (working for free, in their spare time), produced a $300 unmanned aerial vehicle with 90 percent of the functionality of the military's $35,000 Raven. This kind of price reduction is typical of open-sourced projects.

Moreover, conducting bio-security in-house means attracting and retaining a very high level of talent. This puts the Secret Service in competition with industry—a fiscally untenable position—and with academia, which offers researchers the freedom to tackle a wider range of interesting problems. But by tapping the collective intelligence of the life-sciences community, the agency would enlist the help of the group best prepared to address this problem, at no cost.

Open-sourcing the president's genetic information to a select group of security-cleared researchers would bring other benefits as well. It would allow the life sciences to follow in the footsteps of the computer sciences, where "red-team exercises," or "penetration testing," are extremely common practices. In these exercises, the red team—usually a group of faux-black-hat hackers—attempts to find weaknesses in an organization's defenses (the blue team). A similar testing environment could be developed for biological war games.

One of the reasons this kind of practice has been so widely instituted in the computer world is that the speed of development far exceeds the ability of any individual security expert, working alone, to keep pace. Because the life sciences are now advancing faster than computing, little short of an internal Manhattan Project–style effort could put the Secret Service ahead of this curve. The FBI has far greater resources at its disposal than the Secret Service; almost 36,000 people work there, for instance, compared with fewer than 7,000 at the Secret Service. Yet Edward You and the FBI reviewed this same problem and concluded that the *only* way the bureau could keep up with biological threats was by involving the

whole of the life-sciences community.

So why go further? Why take the radical step of releasing the president's genome to the world instead of just to researchers with security clearances? For one thing, as the U.S. State Department's DNA-gathering mandate makes clear, the surreptitious collection of world leaders' genetic material has already begun. It would not be surprising if the president's DNA has already been collected and analyzed by America's adversaries. Nor is it unthinkable, given our increasingly nasty party politics, that the president's domestic political opponents are in possession of his DNA. In the November 2008 issue of *The New England Journal of Medicine*, Robert C. Green and George J. Annas warned of this possibility, writing that by the 2012 election, "advances in genomics will make it more likely that DNA will be collected and analyzed to assess genetic risk information that could be used for or, more likely, against presidential candidates." It's also not hard to imagine the rise of a biological analog to the computer-hacking group Anonymous, intent on providing a transparent picture of world leaders' genomes and medical histories. Sooner or later, even without open-sourcing, a president's genome will end up in the public eye.

So the question becomes: Is it more dangerous to play defense and hope for the best, or to go on offense and prepare for the worst? Neither choice is terrific, but even beyond the important issues of cost and talent attraction, open-sourcing—as Claire Fraser, the director of the Institute for Genome Sciences at the University of Maryland School of Medicine, points out—"would level the playing field, removing the need for intelligence agencies to plan for every possible worst-case scenario."

It would also let the White House preempt the media storm that would occur if someone else leaked the president's genome. In addition, constant scrutiny of the president's genome would allow us to establish a baseline and track genetic changes over time, producing an exceptional level of early detection of cancers and other metabolic diseases. And if such diseases were found, an open-sourced genome could likewise accelerate the development of personalized therapies.

The largest factor to consider is time. In 2008, some 14,000 people were working in U.S. labs with access to seriously pathogenic materials; we don't know how many tens of thousands more are doing the same overseas. Outside those labs, the tools and techniques of genetic engineering are accessible to many other people. Back in 2003, a panel of life-sciences experts, convened by the National Academy of Sciences for the CIA's Strategic Assessments Group, noted that because the processes and techniques needed for the development of advanced bio agents can be used for good or for ill, distinguishing legitimate research from research for the production of bioweapons will soon be extremely difficult. As a result, "most panelists argued that a qualitatively different relationship between the government and life sciences communities might be needed to most effectively grapple with the future BW threat."

In our view, it's no longer a question of "might be." Advances in biotechnology are radically changing the scientific landscape. We are entering a world where imagination is the only brake on biology, where dedicated individuals can create new life from scratch. Today, when a difficult problem is mentioned, a commonly heard refrain is *There's an app for that*. Sooner than you might believe, *an app* will be replaced by *an organism* when we think about the solutions to many problems. In light of this coming synbio revolution, a wider-ranging relationship between scientists and security organizations—one defined by open exchange, continual collaboration, and crowd-sourced defenses—may prove the only way to protect the president. And, in the process, the rest of us.

Andrew Hessel *is a faculty member and a former co-chair of bioinformatics and biotechnology at Singularity University, and a fellow at the Institute for Science, Society, and Policy at the University of Ottawa.*

Marc Goodman investigates the impact of advancing technologies on global security, advising Interpol and the U.S. government. He is the founder of the Future Crimes Institute and Chair for Policy, Law & Ethics at Silicon Valley's Singularity University.

Steven Kotler is a New York Times–best-selling author and an award-winning journalist.

Faster, More Economical Method For Detecting Bioterror Threats

Source: http://www.medicalnewstoday.com/releases/252408.php

Texas Biomedical Research Institute scientists in San Antonio have developed a faster, less expensive route to screen suitable tests for bioterror threats and accelerate the application of countermeasures.

The new process screens for pairs of affinity reagents - molecular magnets that bind to and hold on to their targets, be they toxins, viruses or bacteria. That will enable countermeasures to be selected and utilized much faster than the current practice.

"Using crude extracts from *E. coli*, the workhorse bacterium of the biotechnology laboratory, the new route bypasses the need for purification and complex equipment, enabling screening to be performed in under an hour," said Andrew Hayhurst, Ph.D., a Texas Biomed virologist.

Normally, he said, such screening requires sophisticated costly equipment to purify and analyze the affinity reagents. Such analysis becomes a huge burden when hundreds of reagents need to be checked and can take weeks to months.

The process - funded primarily by Texas Biomed and the San Antonio Area Foundation, and in part by the Defense Threat Reduction Agency and the National Institutes of Health (NIH) - was described online in the November 5, 2012 issue of Nature Publishing Group's *Scientific Reports*.

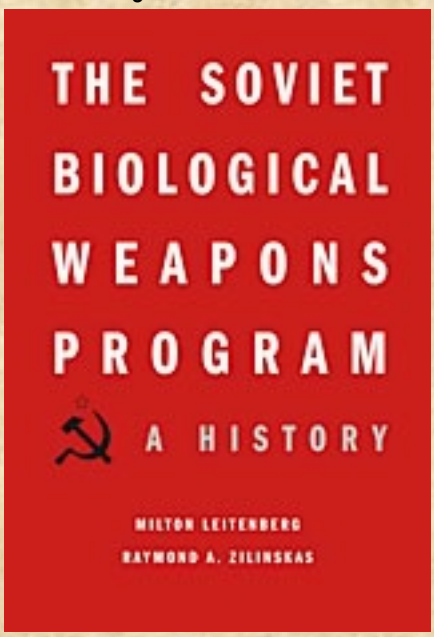
"We need an inexpensive route to screen libraries of affinity reagents. It had to be simple and self-contained as we eventually needed it to work in the space-suit lab or hot zone," said Hayhurst.

His surprisingly simple scheme allows scientists to make stop-gap tests to any given biological threat in a matter of days, with the screening step completed in an hour. The goal now is to speed up

the entire process to work within a single day.
Hayhurst initially developed the pipeline using llama antibodies as the affinity reagents to botulinum neurotoxins, known as the world's most poisonous poisons - 100 billion times more toxic than cyanide and handled in a specialized biosafety cabinet at biosafety level 2. Satisfied that the system was working, he then took it into the biosafety level 4 laboratory with his assistant, Laura Jo Sherwood, and they generated a stop-gap test for Ebolavirus Zaire in days. This virus has been shown to be 95 percent lethal in outbreak settings and with no vaccine or therapeutic it is a risk to the U.S. through importation. Botulinum neurotoxins and Ebolavirus are among a handful of threats now categorized as Tier 1 agents, presenting the greatest risk of deliberate misuse with the most significant potential for mass casualties or devastating effects to the economy, critical infrastructure; or public confidence.
"Being able to respond quickly to known biological threats will better prepare us for combating emerging and engineered threats of the future," Hayhurst said. "However, the great thing about this test pipeline is that it can be applied to almost any target of interest, including markers of diseases like cancer."
Texas Biomed has applied for a patent on the process. It potentially could be licensed to companies for developing diagnostics to specific medical conditions, tests for environmental monitoring, or to accelerate in-house research programs.

The Soviet Biological Weapons Program – A History

By Milton Leitenberg and Raymond A. Zilinskas (Publication July 2012)
Source: http://www.hup.harvard.edu/catalog.php?isbn=9780674047709



Russian officials claim today that the USSR never possessed an offensive biological weapons program. In fact, the Soviet government spent billions of rubles and hard currency to fund a hugely expensive weapons program that added nothing to the country's security. This history is the first attempt to understand the broad scope of the USSR's offensive biological weapons research—its inception in the 1920s, its growth between 1970 and 1990, and its possible remnants in present-day Russia. We learn that the U.S. and U.K. governments never obtained clear evidence of the program's closure from 1990 to the present day, raising the critical question whether the means for waging biological warfare could be resurrected in Russia in the future.
Based on interviews with important Soviet scientists and managers, papers from the Soviet Central Committee, and U.S. and U.K. declassified documents, this book peels back layers of lies, to reveal how and why Soviet leaders decided to develop biological weapons, the scientific resources they dedicated to this task, and the multitude of research institutes that applied themselves to its fulfillment. We learn that Biopreparat, an ostensibly civilian organization, was established to manage a top secret program, code-named Ferment, whose objective was to apply genetic engineering to develop strains of pathogenic agents that had never existed in nature. **Leitenberg** and **Zilinskas** consider the performance of the U.S. intelligence community in discovering and assessing these activities, and they examine in detail the crucial years 1985 to 1992, when Mikhail Gorbachev's attempts to put an end to the program were thwarted as they were under Yeltsin.

"Comprehensive… **Leitenberg** and **Zilinskas** drill deep into the institutional, scientific and personnel factors in the Soviet program… I have a feeling that students of the Cold War will be digging into it for a long time to come."— *David E. Hoffman, Foreign Policy*

"This is the most authoritative and comprehensive account of an important if arcane subject, requiring prodigious research and care in evaluating and verifying official and unofficial reported information. The book does not address the continuing problem of determining current or future compliance or noncompliance with the Biological Weapons Convention by Russia (or others), but it demonstrates the great difficulties in seeking to do so."— *Ambassador Raymond L. Garthoff*

***Milton Leitenberg** is Senior Research Scholar at the University of Maryland.*

***Raymond A. Zilinskas** is Director of the Chemical and Biological Weapons Nonproliferation Program at the Monterey Institute of International Studies.*

Much of the book is devoted to a description of the vast infrastructure of Soviet BW research and production, including descriptions of the various institutes, their history, their workforce and the nature of their research, as far as it could be discerned. Along the way, many fascinating and sometimes horrific topics are addressed. For example:

- In an effort to enhance the weapons-related properties of BW agents, Soviet scientists spent years working to create a viral "chimera," which is an organism that contains genetic material from two or more other organisms.
- Other scientists worked to eliminate the "epitopes" on the surface of existing BW agents in order to make them unrecognizable to regular diagnostic techniques. By using such a modified agent, "the Soviets would have made it considerably more difficult for the attacked population to identify the causative pathogen of the resulting disease outbreak and begin timely treatment."
- A project codenamed Hunter (Okhotnik) sought to develop hybrids of bacteria and viruses such that use of an antibiotic to kill the bacteria would trigger release of the virus. "Unlike other national BW programs, which without exception used only classical or traditional applied microbiology techniques to weaponize agents, the post-1972 Soviet program had a futuristic aspect. By employing genetic manipulation and other molecular biology techniques, its scientists were able to breach barriers separating species…."
- The Soviet BW program appears to have taken advantage of the declassification in the 1970s of a large number of documents from the United States BW program. Thus, the design of the Soviet Gshch-304 BW bomblet was found to closely resemble that of the declassified US E-130R2 bomblet. In 2001, the US Government moved to reclassify many documents on the US BW program, but "nothing could be done about recalling reports that had been distributed relatively freely for more than 35 years."
- The quality of US intelligence about the Soviet BW program left much to be desired. "Intelligence about Soviet BW-related activities is relatively thin for the pre-1972 period; meager and often of dubious value during 1970-1979; and a little less meager and of better quality during 1980-1990." After 1990, little has been declassified. "There is an unknown number of still-classified reports concerning the Soviet BW program produced by the CIA and perhaps by other agencies that we do not have," the authors write. The state of declassification is such that "we have been able to collect far more information" about the history of Soviet BW activities from interviews with former Soviet scientists and others than from declassified official records.
- In what the authors term "a horrendous mistake by the United States," the US government undertook a covert deception and disinformation program aimed at the Soviet Union in the late 1960s which implied falsely that the US had a clandestine biological weapons program. This unfortunate campaign may have reinforced an existing Soviet belief that the US had never terminated its own offensive BW program, a belief that lent impetus, if not legitimacy, to the Soviet BW program.
- Today, the situation with respect to BW in the former Soviet Union is "ambiguous and unsatisfactory," Leitenberg and Zilinskas write. "There remains the possibility that Russia maintains portions of an offensive BW program in violation of the BWC." Alternatively, "since we do not actually know what is and has been taking place within the three [Ministry of Defense BW] facilities since 1992, perhaps the situation is better than might be feared."

domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 8 Issue 10, October 2012

Medical Emergencies

DHS tries monitoring social media for signs of biological attacks

Source: http://www.nextgov.com/defense/2012/11/dhs-tries-monitoring-social-media-signs-biological-attacks/59406/

The Homeland Security Department has commissioned Accenture to test technology that mines open social networks for indications of pandemics, according to the vendor.

The $3 million, yearlong "bio-surveillance" program will try to instantaneously spot public health trends among the massive amount of data that citizens share online daily, company officials said in announcing the deal Thursday.

The business case for the new DHS program has not been proved yet, Accenture officials acknowledged. "Our pilot program seeks to prove this case," said John Matchette, Accenture managing director for U.S. public safety. "In theory, social media analytics would have shown timely indicators for multiple past biological and health-related events."

In July, President Obama issued a national strategy for bio-surveillance that directs federal agencies to think outside the box in detecting incidents. "Consider social media as a force multiplier that can empower individuals and communities to provide early warning and global situational awareness," the guidelines stated.

The strategy cites a number of recent threats to underscore the need for innovative bio-surveillance, including the 2001 anthrax letters, 2003 SARS outbreak, 2009 bird flu pandemic and2011 Japan nuclear emergency.

Arlington, Va.-based Accenture and DHS will develop a model to "manage, link and analyze data from social media networks in real time to better inform and protect the public in the event of a national health emergency such as an infectious disease outbreak or a biological attack," company officials stated. Homeland Security will examine information available through various outlets such as Facebook, Twitter, LinkedIn and blogs, company officials added.

All information "channels are yet to be defined," Matchette said later.

This is not the first time Homeland Security has tracked social media in the interest of public safety. One ongoing project has sparked a lawsuit and vexed some House members.

The Electronic Privacy Information Center has sued DHS for records on search terms and technical tools that officials are using to scour social networks, blogs and online comment threads for terrorist threats. The effort is expected to be undertaken "by individuals who established fictitious usernames and passwords to create covert social media profiles to spy on other users," the center's website states. At a February congressional hearing, House Homeland Security Committee members told DHS officials they worried about the program violating citizens' free speech and constitutional protections against unreasonable searches.

Written testimony from DHS officials stated the department enforces standards to safeguard privacy. Using publicly available search engines and content aggregators, the department reviews information already "accessible on certain heavily trafficked social media sites" for data to establish a common operating picture, without monitoring individuals' comments or collecting personal information -- "with very narrow exceptions," the officials said.

Some diseases designated as "emerging" have been around for centuries

Source: http://www.homelandsecuritynewswire.com/dr20121114-scientists-some-diseases-designated-as-emerging-have-been-around-for-centuries

The Ebola, Marburg, and Lassa viruses are commonly referred to as emerging diseases, but leading scientists say these life-threatening viruses have been around for centuries.

In a perspective in the 9 November issue of the journal *Science*, researchers say it would be more appropriate to refer to these viruses as emerging diagnoses.

"The infectious agents were identified around the middle of the twentieth century but that does not mean that they were new," said Joseph McCormick, M.D., one of the authors of the perspective and regional dean of the University of Texas School of Public Health Brownsville Regional Campus, which is part of UTHealth. "Some of the viruses, including Lassa and Ebola, have been around for thousands of years."

A University of Texas Health Center release reports that the viruses burst onto the scene in the 1960s when outbreaks decimated areas of west and central Africa. The viruses can lead to hemorrhagic fever, a condition characterized by bleeding, shock, vomiting, and diarrhea. In severe cases, the death rate may reach 90 percent.

These viruses thrive in animals — not humans. People, however, can get the viruses if they come in contact with infected animals or are exposed to virus-infected fluids or tissues. Infected people are moderately contagious with person-to-person transmission only through direct contact with infectious fluids such as blood or urine. Patients with Lassa virus can be successfully treated by antiviral medications.

With the aid of epidemiologic, ecologic, and genetic studies, researchers have learned that these viral hemorrhagic fevers are endemic in several areas of Africa. The Ebola viruses are endemic in other parts of the globe.

"The Arenavirus family of viruses that occur on many continents, of which the African Lassa virus is a member, is an ancient family of viruses that have likely evolved along with their rodent hosts over millions of years," said McCormick, former chief of the Special Pathogens Branch of the Centers for Disease Control and Prevention (CDC).

So what would designating the viruses as emerging diagnoses mean?

"It means that these viruses have lurked as enzootic viruses in the environment and that their 'discovery' was related to the scientific capacity to make the diagnosis rather than their 'emergence,'" McCormick said. "However, it also means that we also now know more about the risks of encountering them and therefore, how to identify those who may be at risk for infection."

He said the designation would aid in the diagnosis. "Now that we understand more about their ecological niches and geographical distribution, we know more about how to avoid them. We also know more about how they cause disease and we may be able to improve treatment and seek vaccines.

All of this information will lead to a more proactive approach for detection and prevention," McCormick said. "Antibody tests now allow public health officials to gauge the exposure of the public to these viruses."

With this information, McCormick, the James H. Steele Professor of Epidemiology at the UT School of Public Health, said public health officials could develop strategies for prevention and mitigation of epidemics that have characterized these viruses in the past.

McCormick said that with the ease and rapidity of global transportation, it is also important for caregivers in other parts of the world to familiarize themselves with the signs and symptoms. "The symptoms in the early stages are fever, headache and nausea and can easily be misdiagnosed as the flu," said McCormick, adding that physicians need to ask about the travel history of feverish patients.

McCormick is one of the world's foremost authorities on the Ebola and Lassa viruses. He also led the first HIV investigation in Africa and is the investigator who isolated the oldest HIV strain, which is recounted in the book, *Level 4: Virus Hunters of the CDC*, which he co-authored with Susan Fisher-Hoch, M.D. She is a professor of epidemiology at the UT School of Public Health Brownsville Regional Campus. McCormick and Fisher-Hoch are also on the faculty of

the University of Texas Graduate School of Biomedical Sciences at Houston.

— Read more in Stephen K. Gire et al., "Emerging Disease or Diagnosis?" Science 338, no. 6108 (9 November 2012): 750-52

US to scan status updates and tweets for bioterrorism evidence

Source: http://www.wired.co.uk/news/archive/2012-11/13/scan-social-networks-for-bioterrorism

The US department of Homeland Security has commissioned a one-year contract to investigate the efficacy of using social networks to identify instances of bioterrorism, pandemics and other health and security risks.

It is paying Accenture Federal Services $3 million (£1.8 million) to scan the networks' for key words in real time to see if growing threats or health trends can be distinguished. So if an individual flags up a nasty cough in a Facebook update, for instance, the software will be looking to see if key medical terminology is repeated in connected groups or from other individuals posting from the same location.

"This is big data analytics," said John Matchette, managing director for Accenture's public safety department, who admits the technique is yet to be proven. "In theory, social media analytics would have shown timely indicators for multiple past biological and health-related events." Mobile data mapping has been used in the past to track and predict population movements following natural disasters and algorithms can use data to track disease hotspots after the event. However, this latest experiment could provide real time information to help stem disease spread, develop early warning systems and help emergency services coordinate react in a timely fashion

According to a company statement from Accenture, the software will constantly scan blogs, as well as the usual outlets, but not all networks and channels have been decided upon. It's no surprise that national security departments monitor social networks to look out for threats (Paul Chambers' arrest after a tongue-in-cheek faux bomb tweet threat being a perfect example of when that monitoring goes very wrong), however Homeland Security is already being sued by civil liberties group Electronic Privacy Information Centre and is under pressure to answer questions about setting up fake social networking accounts to search for key words such as "virus" and "trojan". The department has been accused of violating the public's free speech and constitutional protections against unreasonable searches. No one would disagree there needs to be better systems in place to monitor and protect against the spread of infectious disease, however how data is monitored to do this has come under fire.

"The information won't be tracked back to individuals who posted it," stated Matchette.

Not everyone is convinced. "Even when data is in aggregate, we don't have any clear policies around how data will be used and how it can be traced back, including if and when there are signs of an illness outbreak," Deven McGraw, director of the health privacy project at the Centre for Democracy and Technology, told WebProNews. "I think it's a legitimate question to ask [Homeland Security] what the guidelines are for using this data. I'd prefer they have a plan in advance for dealing with this, rather than waiting."

A statement on guidelines from Homeland Security -- which has begun aggregating data from the Centres for Disease Control and Prevention and collecting urban air samples as points of reference -- is somewhat vague, but does admit there is room to home in on specific persons of interest. Information that is already "accessible on certain heavily trafficked social media sites" is analysed without gathering personal specifics on an individual, "with very narrow exceptions".

Global monitoring of infectious diseases in dogs and cats to protect humans

Source:http://www.homelandsecuritynewswire.com/dr20121113-global-monitoring-of-infectious-diseases-in-dogs-and-cats-to-protect-humans

Most emerging infectious diseases of humans come from animals. International health agencies monitor these diseases, but they do so only for humans and livestock, not for companion dogs and cats. A new study recommends a global system is needed to monitor infectious diseases of companion dogs and cats.

The study, led by Michael Day, Professor of Veterinary Pathology in the School of Veterinary Sciences at the University of Bristol and published online in *Emerging Infectious Diseases*, lists key infectious diseases that may be transmitted between dogs and cats and man ('zoonotic diseases'). It is well recognized that most of the major new diseases of mankind will have an animal origin and dogs and cats are a potential source of such "emerging diseases."

A University of Bristol release reports that the World Small Animal Veterinary Association (WSAVA) One Health Committee, which promotes the closer integration of human and animal healthcare ("One Health"), in collaboration with the U.S. Centers for Disease Control and Prevention (CDC), the World Organisation for Animal Health (OIE), and the World Health Organization (WHO), recommends in the paper a coordinated global disease monitoring system is established for veterinarians who work in small companion animal practice.

Development of such a scheme, however, would require significant political will, scientific application, and financial support that could be achieved through a public-private partnership.

The knowledge gained through surveillance would permit more effective global control of small companion animal zoonoses and so reduce the risks inherent within this most fundamental of human relationships.

Canine rabies virus infection, one of the diseases listed in the paper, is estimated to kill a minimum of 55,000 people in Africa and Asia each year.

Michael Day, Professor of Veterinary Pathology in the School of Veterinary Sciences, said: "The number of small companion animals is significant. For example there are an estimated eight to ten million dogs living in up to 31 per cent of U.K. homes and in the U.S., 72 million dogs in 37 percent of homes.

"In developed countries the relationship between man and dogs and cats has deepened, with these animals now closely sharing the human indoor environment. The benefits of pet ownership on human health, well-being and development are unquestionable, but as dogs and cats have moved from the barn, to the house, to the bedroom, the potential for disease spread to humans increases. Control of diseases among dogs and cats is a good way to prevent spread to humans."

Small companion animals, most typically dogs and cats, are kept by people for companionship or a range of utilitarian purposes. Dogs and cats have a close relationship with their human owners and play an important role in the cultures of both developed and developing communities. The social and societal benefits of pet ownership are significant, with dogs now participating in programs in institutions such as schools, prisons and hospitals, in addition to their role in family life.

In human, livestock and wildlife heath there are programs of active surveillance for infectious disease, which monitor the global distribution and movement of key infectious agents. For example, the WHO monitors human influenza virus infection through a network of 111 centers in eighty-three countries. In contrast, there is no such monitoring for the infections that may be transmitted between small companion animals and man.

— Read more in Michael J. Day et al., "Surveillance of zoonotic infectious diseases transmitted by small companion animals," Emerging Infectious Diseases *(26 October 2012*)

Milk offers possible defense against the deadly bioterrorism agent ricin

By Shannadora Hollis

Source: http://www.asbmb.org/asbmbtoday/asbmbtoday_article.aspx?id=18386

What if a simple glass of milk contained the antidote to one of the most deadly toxins known to man? Well, it turns out that this common household beverage, often recognized for its role in promoting strong bones, also may be a strong inhibitor of the highly toxic compound ricin.

Figure 1. *Ricinus communis. Photo from Wikipedia.*

What is ricin?

Ricin is found naturally in seeds of ricinus communis, also known as the castor plant (*see Fig. 1*). The plant is indigenous to the southeastern Mediterranean Basin but is widespread in tropical regions. It produces seeds, or beans (*see Fig. 2*), that when pressed produce an oil. Castor oil has been used in traditional medicine as a laxative and to stimulate full-term labor. While the plant is known for these health benefits, it is also the source of the lethal poison ricin, which remains in the pulp of the seeds after they are pressed. In other words, the plant can heal you or kill you, depending on how it's processed. Ricin is a Category B compound, the second-highest-priority agent class designated by the Centers for Disease Control and Prevention. According to Vern Schramm, professor of biochemistry at the Albert Einstein College of Medicine in New York and a prominent researcher of ricin, "one castor bean contains enough ricin to kill thousands of people."

Figure 2. Castor beans. *Photo from Wikipedia.*

How does ricin work?

Ricin is activated intracellularly by proteolytic cleavage to form the A chain, which has enzymatic activity. The A chain is linked to a B chain by a disulfide bond. The B chain is a lectin that binds carbohydrates such as galactose and galactosamine on the cell surface, facilitating the toxin's entry into the cell by endocytosis (*see Fig. 3 at the end of the text*). Once this happens, ricin is translocated into the cytosol, where the disulfide bond holding the chains together is reduced in the environment of the cell. This releases the enzymatic A chain, which can recognize and cleave a single adenine on the ribosome, the organelle responsible for catalyzing the synthesis of proteins. The enzyme acts like a lawnmower that goes along and cuts one adenine off of every ribosome, leaving inactive ribosomes behind. Within a few hours, the ribosomes in the cell can no longer make protein, and the cell dies. This sequence of molecular

events manifests as organ failure and, finally, death of the organism.

Reported cases of ricin poisoning

While much of the research and speculation around the use of the toxin as a terrorist or warfare agent began in the 1940s, it received a great deal of public attention in 1978. In that year, Georgi Markov, a Bulgarian journalist and vocal dissident of the Communist party, was attacked by a man with an umbrella in London while he was on his way to work. The umbrella had been modified to inject a poison ricin pellet under his skin. Markov died three days later from just a 0.2 milligram dose.

Over the past decade, almost a dozen more cases of ricin possession or attempted poisoning have been reported, including an incident in which several U.S. Senate office buildings were shut down when the toxin was found in 2004 in the office suite of the Senate majority leader, Bill Frist. These incidents have created concern among government and public health officials due to the potential for ricin to be used as a biological weapon. At present, symptomatic ricin poisoning is treated by giving supportive medical care to minimize the effects. Symptoms include difficulty breathing, fever, cough, nausea, tightness in the chest, heavy sweating and pulmonary edema. Unfortunately, no antidote for ricin exists. Therefore, there is a great deal of interest in identifying inhibitors for the castor bean compound.

Recent strides to inhibit ricin

Researchers at the U.S., Department of Agriculture, led by Reuven Rasooly, initially set out to create a method to detect ricin in various foods in hopes of eventually inhibiting its biological activity. However, the group had difficulty detecting ricin in milk. Based on this finding, the team hypothesized that the carbohydrate-binding B chain of ricin was interacting with the galactose present in the milk. This led the researchers to examine ricin toxicity in the widely consumed natural food.

In a recent Journal of Biological Chemistry article by the team, the effect of ricin on living cells was visualized and quantified by measuring the changes in the fluorescence intensity level of the green fluorescent protein reporter in African green monkey kidney cells. The more the cells fluoresce, the more protein is being made by the ribosomes. The effect of milk on ricin post-exposure was mimicked by measuring the amount of bound toxin in the presence of milk after 15 minutes of exposure to the castor bean derivative. According to Rasooly, "this is like a treatment, and you need to do it very soon after you know that you have the ricin [exposure], because when the toxin enters the cell it's too late."

Upon exposure of the cells to the poison, it was determined, milk not only removed bound ricin but also reduced the attachment of the toxin to its receptor by up to 88 percent. Furthermore, the biological activity of 1 ng/ml ricin was completely neutralized in solutions containing as little as 1 percent milk.

The mechanism of ricin inhibition also was elucidated in the study. It was confirmed that milk inhibits ricin activity by competitively binding the B chain lectin of the toxin, making it unavailable to galactoside receptor sites on the cell surface, thus reducing the number of toxin molecules that enter the cell.

What next?

It is important to note that this research was conducted in an in vitro system and, therefore, the results may not apply to living beings. In addition, the information gleaned from this study is on the basis of ricin ingestion and highlights a therapeutic approach that also requires ingestion. On one hand, inhibiting ricin toxicity by using milk is an appealing therapy because "milk is a food that we can find in any grocery store and it has no side effects unless people have allergies," says Rasooly. However, according to Schramm "ricin is not very toxic when it is ingested…because most of the protein is degraded [by digestive enzymes] in the stomach and never gets into the [blood] circulation."

Nevertheless, the finding offers an insightful biological mechanism for how milk acts on the toxin. Schramm goes on to say, "The paper in JBC really shows a way of preventing the action of the native ricin in cases of poisoning. I think the most important part of this paper is that, if you understand the exact carbohydrates that are blocking the action of the ricin B chain on human cells, you might be able to get those into a form that could be injected or inhaled and prevent the toxicity of accidental or intentional bioterrorism releases of ricin."

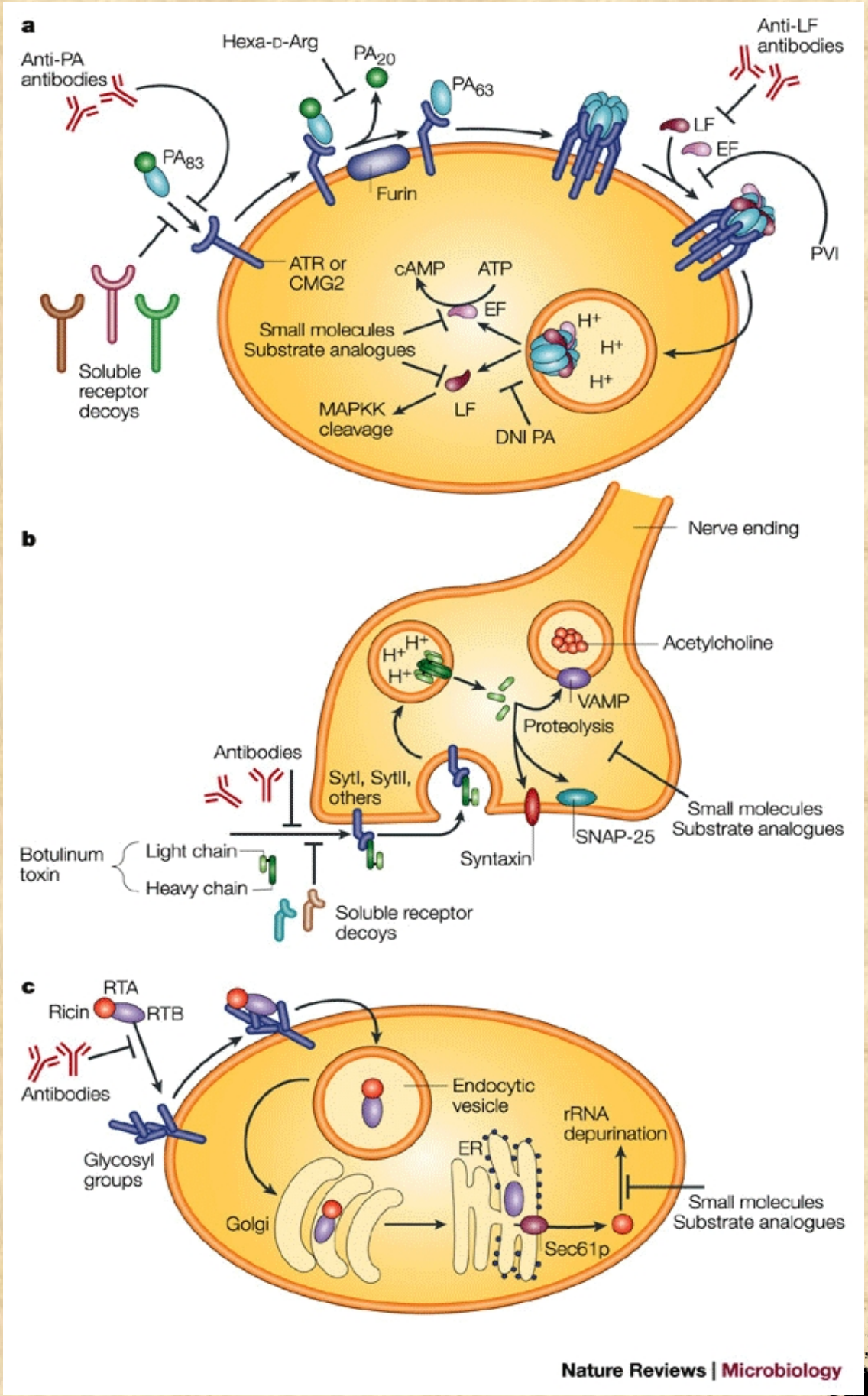

a
Anti-PA antibodies
Hexa-D-Arg
PA20
PA63
PA83
Furin
Anti-LF antibodies
LF
EF
PVI
ATR or CMG2
cAMP
ATP
EF
Small molecules
Substrate analogues
H+
H+
H+
Soluble receptor decoys
MAPKK cleavage
LF
DNI PA
b
Nerve ending
Acetylcholine
H+
H+
H+
VAMP
Proteolysis
Antibodies
SytI, SytII, others
Small molecules
Substrate analogues
SNAP-25
Syntaxin
Botulinum toxin
Light chain
Heavy chain
Soluble receptor decoys
c
RTA
Ricin
RTB
Antibodies
Endocytic vesicle
rRNA depurination
ER
Glycosyl groups
Golgi
Small molecules
Substrate analogues
Sec61p
Nature Reviews | Microbiology

Figure 3 – The pathways for toxin entry into cells and the points at which existing antitoxins can act

a | Anthrax toxin binds to the cellular receptors ATR/TEM8 or CMG2, is processed proteolytically and assembles into a toxin complex. The complex is endocytosed and the active subunits are translocated from the endosome into the cytoplasm, where they can act on their cellular targets. For anthrax toxin, antitoxins are available that can target binding of the toxin to cellular receptors (soluble receptor decoys and anti-PA antibodies), the proteolytic processing (hexa-D-Arg, a furin inhibitor), assembly of the toxin complex (anti-LF antibodies and polyvalent inhibitor, PVI), translocation from the endosome (dominant-negative inhibitor of PA, DNI PA) and the catalytic activity of the toxin on its cellular targets (small molecules and substrate analogues). b | The botulinum neurotoxins (BoNTs) bind to receptors on cholinergic nerve endings, are taken up by endocytosis and translocated from an endosome into the cytosol, where they cleave cellular proteins. Antitoxins are available that inhibit binding to receptors on the nerve endings (antibodies and soluble receptor decoys) and inhibit the proteolytic activity (small molecules and substrate analogues). c | Ricin binds glycosyl groups on lipids and proteins, is taken up by multiple endocytic processes, undergoes retrograde transport through the Golgi apparatus into the endoplasmic reticulum (ER), translocates out of the ER into the cytosol using the Sec61p translocon and modifies its cellular target. Antitoxins are available that inhibit the toxin binding to cellular receptors (antibodies) and block the depurination of ribosomal RNA (small molecules and substrate analogues).

► **Source (figure 3):** http://www.nature.com/nrmicro/journal/v2/n9/fig_tab/nrmicro977_F1.html

Shannadora Hollis *received her B.S. in chemical engineering from North Carolina State University and is a Ph.D. student in the molecular medicine program at the University of Maryland, Baltimore. Her research focuses on the molecular mechanisms that control salt balance and blood pressure in health and disease. She is a native of Washington, D.C., and in her spare time enjoys cooking, thrift-store shopping and painting.*

Ebola may go airborne

Source: http://www.sciencenews.org/view/generic/id/346435/title/Ebola_may_go_airborne

The Ebola virus can spread through the air from pigs to macaques, a new study suggests.

Transmission of the virus — which causes an often fatal hemorrhagic fever in people and primates — was thought to require direct contact with body fluids from an infected animal or person. But in the new study, published online November 15 in *Scientific Reports*, piglets infected with Ebola passed the virus to macaques housed in the same room even though the animals never touched.

"The evidence that the virus got from a pig to a monkey through a respiratory route is good," says Glenn Marsh, a molecular virologist at the Commonwealth Scientific and Industrial Research Organization's Animal Health Laboratory in Geelong, Australia. Marsh was not involved in the new study but has investigated Ebola and other viruses in pigs.

Although pigs transmitted Ebola in the laboratory, there is still no evidence that anyone has been sickened from contact with infected pigs in Africa, where the virus occurs naturally, or that the virus passes through the air under normal conditions, says study coauthor Gary Kobinger, an infectious disease researcher at the University of Manitoba in Winnipeg, Canada. "It's definitely not an efficient route of transmission."

Only 13 of the more than 2,200 human cases of Ebola documented since the virus was discovered in 1976 cannot be traced to direct contact with an infected person, animal or body fluid, he notes. If Ebola were able to spread easily through the air, many more cases might result.

The new study raises questions about whether humans can also transmit Ebola by respiratory routes, says Pierre Formenty, of the World Health Organization's Control of Epidemic Diseases Unit. That is something that will have to be investigated in future outbreaks, he says.

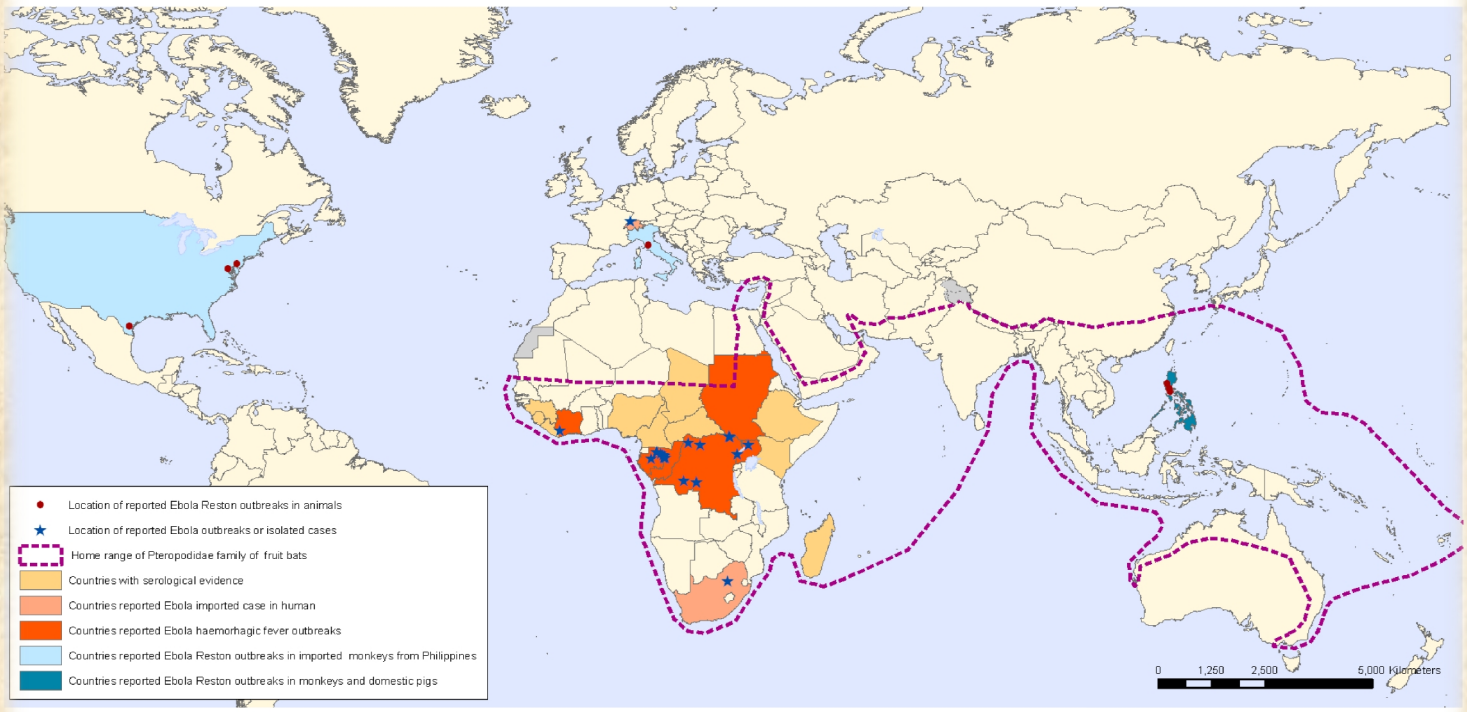
Kobinger became interested in Ebola in pigs after investigating an outbreak in 2007 in the Democratic Republic of the Congo. Villagers mentioned that some pigs had gotten sick and died early in the outbreak. At the time, there was no evidence that Ebola could infect pigs. Kobinger and his colleagues have since

demonstrated that the virus causes disease in pigs in the lab, but no cases have been confirmed in livestock.

"This is all story-telling. Nobody has isolated virus or even detected antibodies from pigs in Africa," Kobinger says.

After about a week living next to infected piglets, two of the macaques fell ill with Ebola. Those two animals were in cages in the path of air flowing from the pigs' enclosure. It took several more days for the other two macaques to develop the disease.

Geographic distribution of Ebola haemorrhagic fever outbreaks and fruit bats of Pteropodidae Family



The boundaries and names shown and the designations used on this map do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.

Data Source: Global Alert and Response Department
World Health Organization
Map Production: Public Health Information
and Geographic Information Systems (GIS)
World Health Organization

World Health Organization

But other researchers discovered that pigs on farms in the Philippines could contract a form of the virus known as Reston Ebola. The Reston strain causes disease in macaques but has not been shown to make people sick. Some pig farmers in the Philippines have antibodies in their blood against Reston Ebola, indicating that infected pigs may have exposed farmers to the virus.

Kobinger wanted to know whether pigs could also pass along the form of Ebola found in Africa. Working in a lab designed to contain the most dangerous pathogens, Kobinger and his colleagues infected piglets with the strain known as Zaire Ebola. The piglets were housed next to four cynomolgus macaques, primates often used as stand-ins for humans. A barrier prevented the animals from coming into direct contact with each other.

While the finding could indicate that the virus spread through the air, the researchers can't rule out that virus may have infected the macaques via water droplets scattered while cleaning the pig cage.

No one is blaming pigs for Ebola outbreaks in Africa now, but Kobinger says the growing pig industry on the continent might want to take a few simple steps to protect their animals. Keeping fruit trees, which attract fruit bats that carry Ebola, away from pig farms is one such measure.

Ebola viruses related to the African strains have been found in orangutans in Indonesia, raising the possibility that other unknown Ebola-like viruses could spill over into pigs and then humans, Marsh says. "That's concerning."

Why typhoid fever pathogen targets only humans

Source: http://www.homelandsecuritynewswire.com/dr20121115-why-typhoid-fever-pathogen-targets-only-humans

"Typhoid Mary" Mallon in forced quarantine in 1907 // Source: commons.wikimedia.org

*Salmonella typhi*is a particularly nasty bacterium that targets only humans and causes typhoid fever, which kills hundreds of thousands of people annually. In a new study appearing in the 16 November issue of the journal *Science*, Yale scientists explain how evolution shaped the pathogen to be so selective.

A Yale University release reports that Jorge E. Galan, the Lucille P. Markey Professor of Microbial Pathogenesis, and colleague Stefania Spano coaxed *Salmonella typhi* to survive within immune cells of mice — a species that in nature cannot be infected with the pathogen. They managed the trick by introducing a single gene from a related strain of Salmonella that can infect multiple species. The gene enable *S. typhi* to destroy a molecular courier known as Rab32, which under normal conditions helps arm anti-microbial defenses against the invader.

In humans, however, the antimicrobial defenses delivered by Rab32 are not effective against *S. typhi*, and this pathogen can establish itself and cause disease.

"The immune system is still firing the bullets, but this pathogen has learned how to dodge them in humans but apparently not in other animals," Galan said.

Unlike the Salmonella bacteria that cause food poisoning, *S. typhi* can be fatal in up to 20 percent of untreated cases. People contract typhoid fever through contaminated food or water, and survivors can sometimes carry the pathogen for years. The loss of a single gene in *S. typhi* gives clues as to why it has lost the ability to replicate in any host other than humans, Galan said.

Deficiencies in the Rab32 surveillance mechanism may also make people more susceptible to leprosy and tuberculosis.

Understanding how the surveillance system works may lead to new strategies to combat a those infectious diseases and help develop new classes of antibiotics to combat pathogens, which are developing resistance to current drugs.

— Read more in Stefania Spanò and Jorge E. Galán, "A Rab32-Dependent Pathway Contributes to Salmonella Typhi Host Restriction," Science 338, no. 6109 (16 November 2012): 960-63

Bioterrorism remains real threat a decade after Anthrax attacks, expert says

Source: http://www.nj.com/news/index.ssf/2012/11/bioterrorism_threat_remains_re.html

Even though the 2001 Anthrax attacks are still commemorated at the Hamilton mail sorting facility that handled at least four letters containing the deadly spores, memory of the bioterrorism campaign that killed five people just weeks after 9/11 has faded in the broader public consciousness.

And that in itself could be dangerous, says Leonard Cole, director of the Terror Medicine and Security program at the University of Medicine and Dentistry of New Jersey, who is scheduled to testify today before the House Homeland Security Subcommittee on Counterterrorism and Intelligence.

Cole (photo), author of the 2003 book, "The Anthrax Letters: A Medical Detective Story," said $60 billion has been spent on measures to combat bioterrorism over the past decade. But spending, like the fear of bioterrorism, has waned after more than a decade without an attack.

"And that certainly does feed into the notion that maybe we ought not to be spending so much," Cole said.

The problem with cutting spending, he said, is the threat of an attack remains real, according to a study he took part in

by a working group of the Aspen Institute, a Washington, D.C. think tank.

"We recognize that there is a continuing serious threat, and that a combination of reasons have let us lower our guard," Cole said, referring to the passage of time and budget constraints.

"We recognize that there is a continuing serious threat, and that a combination of reasons have let us lower our guard"

Cole, who lives in Bergen County, has a diverse resume that includes doctoral degrees in political science and dental medicine. Apart from his UMDNJ post, he teaches political science at Rutgers University. And he has authored or edited 10 books, including the forthcoming, "Local Planning for Terror and Disaster: From bioterrorism to Earthquakes," which he coedited with Nancy Connell, a colleague at UMDNJ.

A terrifying element of the anthrax scare was the elusiveness of the attacker. In 2008, authorities said they were close to indicting a researcher at an Army biodefense lab in Maryland. But the researcher, Bruce E. Ivins, killed himself before charges were filed, and the case was never prosecuted.

In addition to the five people killed in New York City, Washington, D.C., Florida and Connecticut in October and November 2001, 17 others were sickened, including five postal workers in Hamilton. Cole noted another 30,000 people were forced to undergo treatment or take other precautions, while countless others were seized by fear — a reminder that lethality is not the only measure of a terror attack's effectiveness.

"A lot of people, including in official positions, tend to think that an agent would be considered a dangerous weapon depending on how much it kills," Cole said, referring to the variety of pathogens that could be deliberately spread. "But in truth, an agent does not have to kill to be very effective at causing terror, including hysteria, panic, social disruption. And we saw a perfect example of that, just about 11 years ago, with the anthrax letters."

Putting Asia on alert as bioterrorism risk grows

By Jaime Yassif

Source: http://www.scmp.com/comment/insight-opinion/article/1086177/putting-asia-alert-bioterrorism-risk-grows

Looking for an easy-to-reach weekend getaway without the hassle of Chek Lap Kok? As Cecilie Gamst Berg discovers, there's a welcome in the Guangdong hillsides, where visitors are treated like...

A global infectious disease outbreak involving a lethal pathogen - whether spread through a deliberate attack or originating from natural sources - could claim millions of lives and cause severe economic damage. It is essential not only to

mitigate the consequences of a pandemic, but also - with respect to deliberate biological attacks - to minimise the likelihood that it will happen.

An important yet underdeveloped tool for protecting against biological attacks is effective governance of life sciences research. Biotechnology can yield tremendous benefits - including improvements to public health and new sources of energy - but there is also the risk that it will be exploited to develop weapons that target human health. Improved governance can help manage this risk.

A new approach to life sciences governance is needed worldwide, and this issue has particular significance for Asia. The biotech industry, regarded as an engine for growth and job production, has been expanding rapidly in Asia. China, for one, is investing heavily in its domestic biotech industry. Biotechnology in Malaysia reportedly constitutes 2.5 per cent of national economic output, and Indonesia has set its sights on developing robust domestic research and development capabilities in the industry.

In view of this rapid growth, policy and regulatory frameworks to manage the associated risks have to play catch up.

Managing the risks presents several challenges. Firstly, dual-use biotech tools, materials and knowledge are widely distributed, and research takes place at thousands of facilities worldwide. This increases ease of access and hence risk of exploitation by those with malevolent intent.

Secondly, technical barriers are considerably lower for producing an effective biological weapon than for making nuclear weapons, and are well within reach of non-state actors.

Finally, a major concern has been the feasibility of producing a lethal virus from scratch. This capability is presently limited to trained scientists at well-funded research centres, but as technology develops it may become more widely accessible - making it easier to obtain deadly viruses.

More effective management of biosecurity challenges means establishing a culture of responsibility among researchers, developing self-governance practices in the industry, and strengthening institutions to support these efforts.

Many of the tools for life science governance have yet to be developed. This is fertile ground for co-operation across the Pacific.

Jaime Yassif *is a biophysics doctoral candidate at the University of California, Berkeley. Distributed by Pacific Forum CSIS.*

Predicting, preventing, and controlling pandemics

Source: http://www.homelandsecuritynewswire.com/dr20121205-predicting-preventing-and-controlling-pandemics

About **60 percent of infectious diseases are caused by viruses, bacteria**, and other pathogens that make the jump to humans from other species. This includes some of the most devastating disease outbreaks of the past thirty years, including HIV/AIDS, Ebola, and SARS. Despite the huge and rising toll of such diseases, many gaps remain in our understanding of how these "zoonoses" evolve, develop, and spread — gaps that must be filled if we are to succeed in preventing or at least reducing the impact of a next pandemic.

A new paper published in the *Lancet* by Stephen S. Morse, Ph.D., professor of Epidemiology at Columbia University's Mailman School of Public Health, and colleagues, lays out a series of research and surveillance

opportunities that could help bridge these gaps and move the global pandemic strategy from response to pre-emption and prediction. The paper, "Predicting and Preventing the Next Pandemic Zoonosis, is part of a special Lancet series that explores the ecology, drivers, and dynamics of zoonoses with a view toward improving prediction of the next pandemic and reducing the human and economic costs.

A Mailman School of Public Health release reports that according to Morse and the other authors of the Lancet series, there are several stages in disease emergence and each change increases the likelihood of the pathogen making contact with humans. The spread of zoonoses is strongly affected by such human activities as global travel, changes in land use, and animal agriculture. Thus prevention will require intervention and planning on many fronts.

Recent developments in modeling and technology, including revolutionary advances in communications, database design, and use of the latest molecular screening methods to identify previously unknown infectious agents, have put us on the verge of being able to predict the next zoonotic pandemic, according to Morse, who is also co-director of the PREDICT project of the USAID Emerging Pandemic Threats (EPT) Program. Launched in 2009 The PREDICT project is active in twenty developing countries in emerging infectious disease hotspots and focuses on surveillance at human–animal interfaces where cross-species transmission is most likely, often identified through risk or "hotspots" modeling. An essential objective is also building capacity by partnering with local scientists and institutions. Serious deficiencies remain, however — in disease surveillance, in our understanding of the key groups of animals that spread zoonotic disease, and in our ability to analyze the results of these advanced technologies in order identify which pathogens represent a potential threat and which are harmless.

"There is no question of whether we will have more zoonotic pandemics – the question is merely when, and where, the next pandemic will emerge," says Morse. "The challenge now is to establish whether and how researchers can intervene before a pathogen reaches the human population and develop appropriate triggers for action. Zoonotic diseases, by definition, should be a key mission of human health agencies, agricultural authorities and producers, and natural resource managers, all working cooperatively.

In reality, however, the current situation leaves much to be desired, and we need substantial investments in each of these areas."

The release notes that the *Lancet* Series is published ahead of a special 20th Anniversary Symposium to be held on 11-12 December 2012 in Washington, D.C., and hosted by the Institute of Medicine's Forum on Microbial Threats.

In addition to covering the latest research, this year's symposium will take a retrospective look at the IOM's seminal reports on Emerging Infections (1992) and Microbial Threats to Health (2003) as well as the 1996 creation of the Forum. Morse is a member of the original IOM committee on emerging infections and will take part on two panels at this year's Symposium including one on New Initiatives in Surveillance.

"No emerging infection has ever been predicted before it appeared in humans," notes Morse. "That's why developing a global early warning system was a key recommendation of the IOM report and of every expert group. With new technologies, for the first time in history we are now poised to predict and prevent emerging infections at the source, before they reach us. But we're in the very early stages of learning how to use these new capabilities."

— Read more in Stephen S. Morse et al., "Prediction and prevention of the next pandemic zoonosis," The Lancet 380, no. 9857 (1 December 2012): 1956-6

NEW BOOK – Biopreparedness and Public Health: Exploring Synergies

Source: http://link.springer.com/book/10.1007/978-94-007-5273-3/page/1

Edited by: Iris Hunger, Vladan Radosavljevic, Goran Belojevic and Lisa D. Rotz
Springer Netherlands (**2013** - Print ISBN 978-94-007-5272-6)

Preface

The threat from the terrorist use of pathogens has been a major security concern in recent years, articularly after the anthrax letter attacks in the USA in 2001. This threat of intentional outbreaks of diseases stands side by side with the constantly changing natural threat from diseases, epidemics, and pandemics, as illustrated in recent years by the H1N1 in fl uenza pandemic, the SARS outbreak, and the H5N1 avian in fl uenza event. While naturally occurring diseases – both newly emerging and well-known ones – claim the life and health of many people year after year, bioterrorism events have so far had a very limited health impact.

Protection, prevention, and response measures for natural disease outbreaks and for bioterrorism events differ greatly between countries. At the national level these aspects all too often are handled by different actors with different approaches under different funding arrangements. In many states, resources and political attention are so stretched that the bioterrorism threat is not dealt with at all. While natural and deliberate outbreaks of disease differ in a number of ways – e.g., the types of diseases involved, risk communications, or the legal follow-up – in many areas the differences are likely to be small, in particular those involving nondisease-specific public health detection and response activities. Finding these areas of overlap, identifying the differences and the gaps in preparedness measures, and thereby contributing to streamlining response measures so as to enable them to protect public health from all three types of biological threats – natural, accidental, deliberate – is an urgent need for countries worldwide, and in particular for countries whose public health systems are already overburdened by natural disease response.

To address the issue, 34 experts from 17 European countries, including Turkey, as well as the USA, Israel, the World Health Organization, and the European Centre for Disease Prevention and Control gathered for a NATO-sponsored Advanced Research Workshop entitled “Exploring synergies between bioterrorism preparedness and general public health measures” in the Serbian Academy of Sciences and Arts (SANU) in Belgrade, Serbia, during 15–17 November 2010.

In addition to the 34 workshop participants, the fi rst half-day of the workshop, with introductory and more general presentations, drew a number of local experts, illustrating the interest in the issues under discussion. Most notably, the workshop participants welcomed Zoran Jeftic, State Secretary from the Serbian Ministry of Defence, and Lee Litzenberger, Deputy Head of Mission of the US Embassy in Belgrade, who addressed the gathering during the opening ceremony.

The workshop focused on Southeastern Europe, a region where some of the diseases caused by agents of bioterrorism concern, such as tularemia or certain types of hemorrhagic fevers, are endemic. This region also regularly experiences natural outbreaks of other diseases whose causative agents also have relevance as potential bioweapons risk agents. The workshop was not only an opportunity to learn from local experiences in fi ghting these diseases, but also a unique occasion for regional and global networking.

The workshop addressed the current level of threat from naturally occurring infectious diseases and the current bioterrorism threat, the response and preparedness efforts in different countries of Southeastern Europe, France, Germany, Israel, Poland, the United States, the European Union, and globally. From these empirical data, commonalities, differences, and

gaps among states' efforts and between general public health measures and biopreparedness were extracted and discussed. Lessons were derived on where bioterrorism preparedness and response measures at the moment and in the future can bene fi t other areas of public health and vice versa.

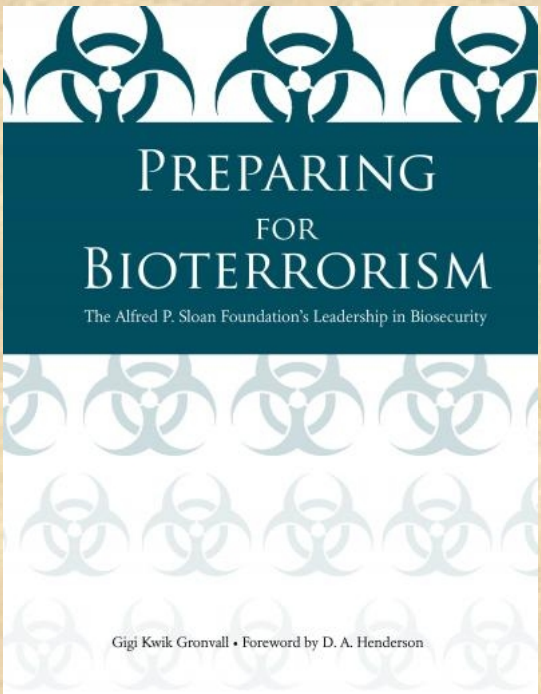
To capture the information that was exchanged during the workshop and further explore synergies for public health preparedness, selected workshop participants were asked to write detailed case studies on the relationship between biopreparedness efforts and other public health measures in their countries or their international organizations, which – together with a number of chapters on more general bio-threat related topics – are assembled in this international scienti fi c monograph.

The thanks of the editors of this volume go to NATO's Science for Peace and Security Programme for funding the original workshop, to the Serbian Academy of Sciences and Arts (SANU) – and in particular to Academician Prof. Ljubisav Rakic – for hosting the workshop in Belgrade, and to two external reviewers who contributed valuable comments during the preparation of this book – **Brig. Gen. (ret) Mario Stefano Peragallo, MD,** Consultant in Preventive Medicine and Hygiene, Italian Army Medical Research Center, Rome (Italy), **and Brig. Gen. (ret) Ioannis Galatas, MD,** Consultant in Allergy and Clinical Immunology, Medical/Hospital CBRNE Planner, and Senior Asymmetric Threats Analyst, Athens (Greece).

Iris Hunger
Carl Friedrich von Weizsäcker Centre for Science and Peace Research; University of Hamburg, Hamburg, Germany.
Vladan Radosavljevic
Military Academy, University of Defence, Belgrade, Serbia.
Goran Belojevic
Institute of Hygiene and Medical Ecology, Faculty of Medicine; University of Belgrade, Serbia.
Lisa D. Rotz
Centers for Disease Control and Prevention, Atlanta, Georgia, USA.

Preparing for bioterrorism

Source: http://www.eurekalert.org/pub_releases/2012-12/cfbo-pfb121112.php



A new book, Preparing for Bioterrorism, written by Gigi Kwik Gronvall and published by the Center for Biosecurity of UPMC, tells the story of some of the important biosecurity projects funded by the Alfred P. Sloan Foundation and how they left the nation better prepared to deal with bioterrorism. Each project is its own story in the book. What emerges is a history of the past decade of progress in biosecurity preparedness in communities across the country and around the world.

Before 9/11 and the anthrax letter attacks, the US government was mostly concerned about biological attacks on the military, on soldiers—it was not prepared for attacks on civilians. Few had seriously planned for such a biological threat, and there was certainly no multidisciplinary community devoted to improving biosecurity.

The Alfred P. Sloan Foundation identified this as a critical gap. In

2000 they started funding projects in civilian preparedness and built a network of experts who were working through these problems. Before biosecurity even existed as a professional field, they were in a good position to put their resources and knowledge to work. Over the next 10 years, Sloan would award more than $44 million in grants in the field of biosecurity. Those grants changed the US strategic direction.

Author Gigi Kwik Gronvall, Senior Associate at the Center for Biosecurity of UPMC, chronicles Sloan's leadership in the field and the innovations that followed to show how the foundation helped lay the groundwork on which US civilian biosecurity has been built.

Who should read this? "Anyone who is interested in or works in biodefense and civilian preparedness," says Gronvall. "There is a lot of history in there, and people will learn why things are the way they are and also why preparedness is something that needs to be continually worked on over time."

"I hope other people will read this as a guidebook on how to effect real, positive change in government," she adds. "Because of Sloan's unique management style, and their commitment to try a range of ideas to see what would work, they provide a good tutorial for how to harness the passion, commitment, and energy of a diverse group of experts. And it worked. We have a way to go, but the US is much better prepared for a biological attack than it was in 2001."

► Read a sample below:

Introduction – Finding a Sustainable Approach to Biosecurity

Sloan Foundation initiatives called attention to the threat of bioterrorism, paved the way for new directions in research, led to new and practical response capabilities, and helped point the US government in the right policy direction.

In October 2000, the Alfred P. Sloan Foundation took on the mission of reducing the threat of bioterrorism. Over the ten years that followed, the foundation triggered fundamental improvements in US preparedness for bioterrorism and naturally occurring diseases. The investments in preparedness were prescient, as the first were made before the anthrax letter attacks in October 2001, and over time, they established the Sloan Foundation as the primary US and international catalyst for innovative thinking and action in biosecurity. This book describes key projects, campaigns, and organizations underwritten by Sloan during its decade in biosecurity and shows how the foundation influenced and shaped the field. The individual projects recounted illustrate how Sloan's work helped to shift thinking about biosecurity by affirming it as a societal responsibility that extended beyond the bounds of the military alone. The project descriptions also illustrate how the foundation's work led to creation of a multidisciplinary professional field of research and practice in biosecurity. In all, this book shows how the nation is more prepared now than it was in 2000 to face natural or deliberate infectious disease threats, an achievement that the Sloan Foundation's support helped bring about.

In 2000, when the Sloan Foundation started its work in biosecurity, civilian biodefense was a nascent concept. Though the consequences of bioterrorism could be terrible numerous deaths, widespread illness, societal and economic disruption, loss of trust in the government community, state, and local preparedness planning was minimal. Most US government biodefense expertise resided in the military and was focused on defending troops from biological warfare because the threat to civilians had not yet been recognized. Relatively few people in the government were thinking about what would happen if a terrorist used anthrax to attack a US city or if smallpox re emerged as a weapon after having been eradicated from the natural world.

Lack of US government preparedness was the prime motivator that moved Ralph E. Gomory, president of the Sloan Foundation from 1989 to 2007, to adopt biosecurity as a mission. In fall 2000, Gomory heard a US government official describe the national strategy to defend against a bioterrorist attack, the centerpiece of which was developing a vaccine from scratch, and then mobilizing rapidly to vaccinate the threatened population. Gomory had no experience in developing or delivering vaccines he came to the Sloan Foundation from IBM, where he had been director of research and then senior vice president for science and technology, but his long experience with a large research organization told him that the government strategy was wishful thinking. He decided that the Sloan Foundation had to act to reduce the threat of bioterrorism. He was already convinced that biological weapons would be a problem in the future because this threat was the result of technological change, and biotechnologies were getting increasingly easier to misuse: "This new technology, widely diffused, will get into the hands of extremist groups."

Gomory tapped Paula Olsiewski, a biochemist and president of a technology consulting company, to direct Sloan's new biosecurity initiative. Olsiewski saw herself as a connector who could "engage as many people as possible to work on different parts of the problem." As such, she reached across

institutional boundaries to convene experts who had never met but were natural allies because their work had the common goal of protecting citizens. She introduced building engineers to police officials, legal scholars to public health officials, and business owners to laboratory scientists. She organized working dinners where people discovered they had common cause with experts from diverse fields and ended up as close collaborators.

Gomory's approach to biosecurity was to "try everything" that could address the problem. Unlike government funders, Sloan did not issue requests for proposals and then wait for good ideas to come to them. Olsiewski searched for people to pursue projects in the areas that she and Gomory decided were important. The foundation did not dictate projects for grantees or require adherence to specific project deliverables. Instead, Gomory and Olsiewski found people who were passionate about their work, shared Sloan's goal of reducing the threat of bioterrorism, understood the changing conditions of the field and the political landscape, and were nimble enough to adjust projects as needed. The foundation's review process was swift and efficient, and numerous projects were funded to see what could work. Gomory and Olsiewski believed that even if an approach was not successful, important lessons could be learned from the experience and applied to other efforts.

From the beginning, it was clear that civilian resilience to bioterrorism would improve only if established institutions and professional communities came to understand and accept new roles in national security. Through targeted grants, Sloan raised awareness of the consequences of bioterrorism for many professional communities and brought experts from multiple disciplines into the field. This was particularly important for healthcare and public health practitioners on the front lines, who would be the first to see victims who were sick with unusual infectious diseases.

Other professions also had to take on new roles to meet the challenges of biosecurity. Sloan funded education programs for scientists and scholarly analyses to encourage life scientists to examine how their training and work could be misused to create biological weapons. Business leaders and building owners were engaged in discussions of ways to protect building occupants from biological agents by improving HVAC systems, planning for pandemic flu, or devising systems to deliver vaccines to employees. Recognizing that law enforcement organizations had limited knowledge about bioterrorism, Sloan funded education programs that encouraged scientists and law enforcement officials to work together, which built trust between the two groups. Finally, Sloan supported many projects designed to reach and engage those policymakers well positioned to influence civilian biodefense policy and make badly needed reforms to public health law and public health preparedness.

The Sloan Foundation jump started interest in civilian biodefense among many previously uninvolved professions and brought those groups together to create a vibrant multidisciplinary field. After 9/11 and the anthrax letters, the fact that Sloan was already investing in biosecurity helped to propel initiatives forward on a nationwide scale and provided a community for those who were interested in contributing their expertise. The foundation funded numerous conferences and events where people shared ideas and learned from one another. Those exchanges led to cross pollination of ideas. In 2000, there were no national conversations about civilian biodefense; by 2003 there was a peer reviewed journal dedicated to biodefense and biosecurity, and now there are a variety of annual conferences and meetings.

Sloan's goal of reducing the threat of bioterrorism was ambitious, but the foundation's approach was pragmatic. Gomory and Olsiewski were interested in solutions that took advantage of existing systems and solutions that people could implement on their own. For example, for influenza preparedness, Sloan invested in studies to determine whether wearing masks or maintaining distance from social contacts could decrease the spread of flu. They funded projects that assessed whether HVAC filtering systems already installed in commercial buildings could be converted from potential pathogen distributors to pathogen filters. Sloan also wanted to harness information already being collected about numbers of hospitalizations, over the counter drug purchases, and school absenteeism to find indications of a bioweapons attack. This commonsense approach guided the foundation to choose projects focused on developing sustainable, affordable ways to protect the US population.

Responsibility for biosecurity is now largely vested in the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) and its internal agencies the Centers for Disease Control and Prevention (CDC), the National Institutes of Health (NIH), and the Food and Drug Administration (FDA) in addition to programs headed by the Department of Defense (DOD). These agencies are responsible for preparedness, response, and recovery, which entails planning response; detecting a biological attack; developing, procuring, stockpiling, and delivering medical countermeasures; communicating with the public; preparing hospitals; attributing an attack; and leading recovery after an event.

Change has occurred in officials' attitudes and beliefs about the public's response to terrorism and disasters. Fears of public panic have been replaced by confidence in the wisdom of giving people as much information as possible about the dangers they face and the actions they can take to protect themselves, their families, and their communities. That confidence is grounded in results of research sponsored by Sloan and others demonstrating that fears of public panic were unfounded. That research also made clear that giving the public as much information as possible is essential because people could be on their own for hours or even days after a

disaster and would need to know what to do during the time before official responders arrive. This attitudinal sea change has produced a widespread commitment to engaging the public in planning and response.
Sloan funding gave researchers the independence they needed to seek creative solutions to biosecurity problems and to criticize government decisions. Sloan funding made some projects easier, if not possible in the first place. The foundation funded projects that the government probably would not have funded during the decade of the foundation's involvement or now as budgets are shrinking across all levels of government. The foundation was more flexible and responsive than government funding agencies can be. And, importantly, Sloan funded work that called attention to areas neglected for many years by the US government.
The Sloan Foundation closed its biosecurity program in 2010 after many successes. During its decade in the field, Sloan awarded more than $44 million in grants to individual researchers, organizations, universities, and government offices. Over that period, US government funding for biodefense grew from $50 million in 2000 to more than $1 billion in 2010. Many of the ideas and practices developed by Sloan grantees, such as civilian preparedness, have been institutionalized, and biosecurity as a multidisciplinary field has been firmly established.
The Sloan program ended during an economic downturn, when budget cuts began to threaten progress in biosecurity. The effects can be seen in cuts to the US public health system that are undermining preparedness systems set up after 9/11. When public health systems are working, they are largely invisible, but as political commitment to those systems wanes and funding is cut, the nation's ability to protect people from the consequences of any type of epidemic will be severely weakened. That will be noticed.
Sloan's legacy is impressive. Beyond all advances in preparedness, a field of practice and research exists that did not in 2000. A substantial body of knowledge has been created. Leaders emerged who are now mentoring and educating the next generation. Laws and public policy have been created or modernized. Many of the programs spearheaded with Sloan Foundation funding will endure and expand. The pursuit of this mission must continue.
In describing this mission, Gomory said that "reducing the threat from bioterrorism is difficult, expensive, and perhaps unruly. But it has to be done. Bioterrorism is something you cannot wish away." Sloan Foundation initiatives called attention to the threat of bioterrorism, paved the way for new directions in research, led to new and practical response capabilities, and helped point the US government in the right policy direction. As the threat of bioterrorism continues to evolve and change, pushed along by international politics and trends in the biological sciences, the field needs a new infusion of energy and support such as the Sloan Foundation provided for so long. The next chapter in this unruly endeavor remains to be written.

Full book available at:
http://www.upmc-biosecurity.org/website/resources/publications/2012/2012-12-12-prep_bioterrorism.html#pdf

Pentagon, NIH fund pollen-based vaccine delivery research

Source: http://www.nextgov.com/health/2012/12/pentagon-nih-fund-pollen-based-vaccine-delivery-research/60064/

The U.S. government in recent months has committed nearly $2 million for research that could one day allow troops in the field to vaccinate themselves against biological warfare threats.

At the core of the Texas Tech University work on improved vaccine delivery is pollen -- the allergy-provoking powder released by flowering plants.
A television commercial provided the spark for the project's inception three years ago, said lead researcher Harvinder Gill, a chemical engineer who specializes in vaccine and drug delivery at the Lubbock institution.

"I was basically passing by the television and I saw these nicely shaped particles on the TV screen," he told *Global Security Newswire* on Friday. "I didn't know what it was. I just stopped and realized it's actually an advertisement for an anti-allergy drug to treat pollen allergies."
Manufacturing synthetic versions of such particles is difficult. Even though the pollens depicted in the commercial "were causing allergies, I wondered if I could use them for a different application, which is to deliver drugs

and vaccines into the human body," Gill said.

Since then, Gill and his colleagues have determined that the allergens within pollen particles can be chemically removed and replaced with a test vaccine. The particles have a hardened shell that would allow the treatment to survive the trip through the stomach and into the intestines to provide protection against infection, Gill said.

The researcher said he believes vaccine-carrying pollens could be delivered via pills or liquids. An oral delivery system offers a number of potential benefits over injections, according to the Pentagon's Defense Advanced Research Projects Agency.

Rather than requiring shots administered by medical professionals, pills could simply be easily swallowed without pain or hassle even in far-off deployment spots. The drugs could also be more easily shipped to troops in the field than liquid vaccines, the agency said in a Nov. 27 press release announcing Gill as a recipient of a DARPA Young Faculty Award.

"Soldiers could really carry them with them or it could be para-dropped in different locations," Gill said. "Those are just advantages … the armed forces could envision getting."

The benefits might also extend to the civilian population, he added. "It is child-friendly, patient-friendly. A lot of disadvantages of vaccinations go away suddenly," Gill said.

The Defense Department office provided Gill's team with $300,000. In September, the researchers received $1.5 million over five years from the National Institutes of Health to continue the project.

The Pentagon office said an orally delivered vaccine could be used against any number of diseases but did not offer specifics. The agency did not respond to requests for further information on its funding of Gill's work.

"By using different combinations of pollens we might be in a position to deliver most vaccines," according to Gill.

Unlike a vaccine administered by injection, a treatment that is ingested could increase mucous membrane immunity in the lungs and intestines, preventing infection from starting in those key bodily systems and then spreading.

The test vaccine carried by pollen particles showed "fantastic" results in producing disease-fighting antibodies in test mice, Gill said.

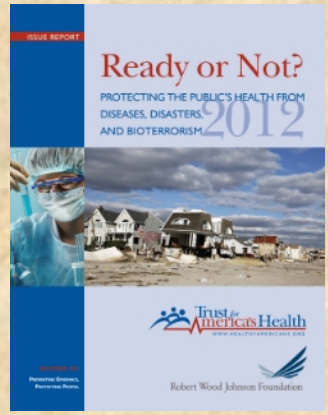
Texas Tech has submitted an application for one patent related to the research and intends to seek another, according to a university press release.

Gill acknowledged that it would require years of research and testing before the work leads to a product that might be available to the military or civilians.

"We want to understand how it's working," he said. "We basically tried it and it worked. We need to now understand how the immune response is working."

Ready or Not? Protecting the Public from Diseases, Disasters, and Bioterrorism

Source: http://www.rwjf.org/en/research-publications/find-rwjf-research/2012/12/ready-or-not-.html

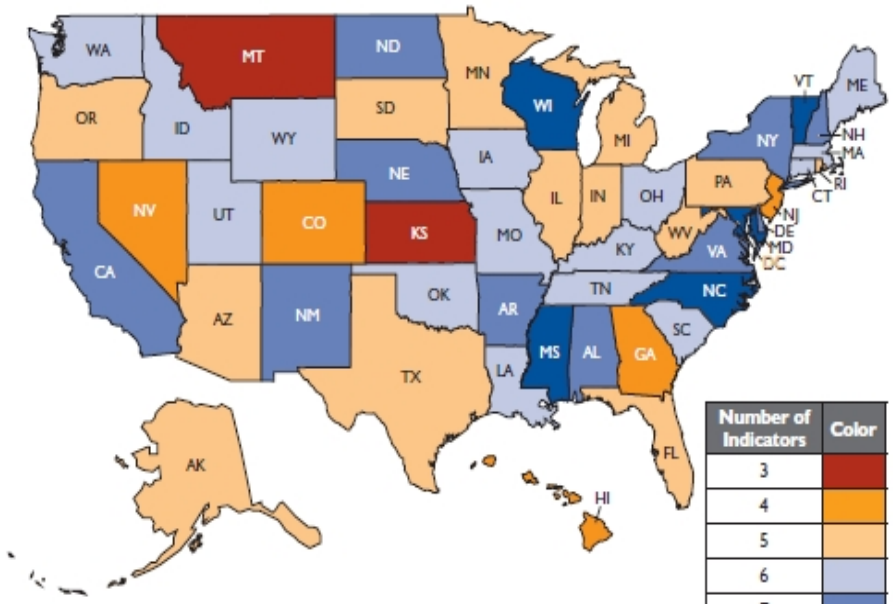


In the 10th annual *Ready or Not? Protecting the Public from Diseases, Disasters, and Bioterrorism* report, issued by the Trust for America's Health (TFAH) and Robert Wood Johnson Foundation (RWJF), 35 states and Washington, D.C., scored a six or lower on 10 key indicators of public health preparedness.

The report found that, while there has been significant progress toward improving public health preparedness over the past 10 years, there continue to be persistent gaps in the country's ability to respond to health emergencies, ranging from bioterrorist threats to serious disease outbreaks to extreme weather. Many of these gaps are due to budget cuts and capacity challenges.

"Public health preparedness has improved leaps and bounds from where we were 10 years ago," said Paul Kuehnert, MS, RN, director of the Public Health Team at the Robert Wood Johnson Foundation. "But severe budget cuts at the federal, state and local levels threaten to undermine that progress. We must establish a baseline of 'better safe than sorry'

preparedness that should not be crossed."



8 (5 states)	7 (10 states)	6 (15 states)	5 (13 states & D.C.)	4 (5 states)	3 (2 states)
Maryland	Alabama	Connecticut	Alaska	Colorado	Kansas
Mississippi	Arkansas	Idaho	Arizona	Georgia	Montana
North Carolina	California	Iowa	D.C.	Hawaii	
Vermont	Delaware	Kentucky	Florida	Nevada	
Wisconsin	Nebraska	Louisiana	Illinois	New Jersey	
	New Hampshire	Maine	Indiana		
	New Mexico	Massachusetts	Michigan		
	New York	Missouri	Minnesota		
	North Dakota	Ohio	Oregon		
	Virginia	Oklahoma	Pennsylvania		
		South Carolina	Rhode Island		
		Tennessee	South Dakota		
		Utah	Texas		
		Washington	West Virginia		
		Wyoming			

Key Findings:

- Twenty-nine states cut public health funding from fiscal years (FY) 2010-11 to 2011-23, with 23 of these states cutting funds for a second year in a row and 14 for three consecutive years. In addition, federal funds for state and local preparedness have decreased 38 percent from FY 2005-2012 (Centers for Disease Control and Prevention (CDC) funds, adjusted for inflation). States are reporting that gains in public health preparedness achieved in the past decade since September 11, 2001, are eroding, and since 2008, budget cuts have resulted in more than 45,700 job losses at state and local health departments.
- Only two states have met the national goal of vaccinating 90 percent of young children, ages 19-36 months, against whooping cough (pertussis). This year Washington state has seen one of the most significant whooping cough outbreaks in recent history.
- Thirty-five states and Washington, D.C., do not currently have complete climate change adaptation plans, which include planning for health threats posed by extreme weather events.
- Thirteen state public health laboratories report they do not have sufficient capacity to work five 12-hour days for six to eight weeks in response to an infectious disease outbreak, such as novel influenza A H1N1.

Around 150 passengers hit by norovirus on Queen Mary 2 during luxury Christmas cruise

Source: http://www.dailymail.co.uk/news/article-2253996/Around-150-passengers-hit-norovirus-Queen-Mary-2-luxury-Christmas-cruise.html

Hundreds of passengers on a luxury Christmas cruise aboard the Queen Mary 2 have been struck down by the winter vomiting bug, it has emerged.

Around 200 of the 2,600 holidaymakers on Cunard's flagship £550million ship have been reportedly taken ill by the infectious norovirus.

Many paid more than £5,000 each for the 13-night tour of the Caribbean on the world's biggest ocean liner, which left New York on Saturday.

But last night guests revealed there was a 'less than festive' feel to the cruise after guests started being sick and suffering diarrhoea within hours of leaving port.

They said they were unable to shake hands with fellow guests on Christmas Day to wish them a Merry Christmas, and those attending church services were given Holy Communion by a vicar in gloves.

One female passenger told the Daily Mail that passengers were unhappy that there were reportedly cases on board the liner before she reached New York, which suggested it had not been properly cleaned prior to holidaymakers embarking.

'The mood is very sombre, it's not the Christmas atmosphere we were hoping for,' the guest said.

'There is a sense of foreboding, with everyone worried that they will be next to come down with the illness.

'The crew are trying their best, continually washing down handrails and lifts, but more cases are being reported each day, it's not at all enjoyable.'

Last year the ship, known as the 'queen of the seas', was branded 'filthy' by US sanitation inspectors following a spot check.

They found 'extremely dirty' water and floor tiling in the splash pool, a human hair in the ice machine and live fruit flies and cockroaches in a storage locker on board.

Those diagnosed with the illness have been quarantined to their cabins, while other passengers have been encouraged to only eat in the main dining room or order food to their rooms.

All salt and pepper shakers have been removed from tables and butter is being served in covered packets.

Shops on board have been told to remove make-up samples and any other promotional purchases or gifts which could be handled by customers.

The liner is currently in the Dominican Republic and is due to make stops in St Lucia, Barbados and St Kitts, before returning to New York on January 4.

While passengers claim hundreds of people have been affected, a spokeswoman for Carnival, which owns the 1132ft-long ship, said there were just 18 people with 'active symptoms' on board yesterday.

She said there had been 'no raised levels' on the previous cruise, but later admitted that around five per cent - 130 - current passengers had already been affected.

They have been asked to comply with doctors' orders, by staying inside their cabins, ordering food via room service and not going on trips ashore, she added.

'Enhanced sanitation protocols have been employed to help minimize

transmission to other passengers,' Michele Andjel, spokeswoman for Carnvial, said.

'The safety and comfort of passengers and crew is always our number one priority.

As is currently standard procedure across our fleet, all the ship's passengers were provided with a precautionary health notice advising of widespread norovirus activity and the health measures to avoid contraction and spread, both on board and whilst ashore.'

The Queen Mary II is the largest and most expensive ocean liner ever built. She entered service in January 2004 and her facilities include fifteen restaurants and bars, five swimming pools, a casino, a ballroom, a theatre, and the first planetarium at sea.

Passengers on the liner are the latest cruise ship guests to be struck down by the vomiting bug.

A fortnight ago the Daily Mail revealed how hundreds of passengers on a tour of European Christmas Markets threatened to stage a sit in after their P&O cruise was plagued by the virus.