POLITICS

Hacking the President's DNA

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.

ANDREW HESSEL, MARC GOODMAN, AND STEVEN KOTLER

NOVEMBER 2012 ISSUE

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 (a k a "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.

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

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.

We want to hear what you think. Submit a letter to the editor or write to letters@theatlantic.com.