Global Security

Benjamin Wittes

1 Introduction

In 1914, in the wake of the assassination of Archduke Franz Ferdinand, a foreign affairs writer named F. Cunliffe-Owen looked for the bright side. "While it is only natural that one should be stricken with horror at the brutal and shocking assassination," he wrote in the *New York Sun*, "it is impossible to deny that [the archduke's] disappearance from the scene is calculated to diminish the tenseness of the [general European] situation and to make peace both within and without the dual empire." The archduke was so universally regarded as a "disturbing factor and as committed to forceful and aggressive policies," he added, "that the news of his death is almost calculated to create a feeling of universal relief" (Cunliffe-Owen 1914).

For anyone undertaking the project of imagining global security over the course of the coming century, poor Mr. Cunliffe-Owen's article – and the many hundreds of others like it that, across time and subject matter, have gotten big questions spectacularly wrong – is a cautionary tale with a loud moral: Predicting the future offers many more opportunities to look stupid than to look prescient. Even with a horizon of just a few weeks, Mr. Cunliffe-Owen managed to misinterpret the triggering event for World War I – which was kind of a big event in the history of global security – as one of those moments of sudden relaxation that lets us all breathe a little easier. And it wasn't that he was an idiot, either; in fact, he appears to have been a well-respected foreign policy analyst. If he couldn't anticipate the coming month within 180 degrees of the right direction, one should probably begin with a certain degree of humility in anticipating the next 100 years.

The future of global security is one of those ultimate multivariate equations – one with few constants, a huge number of variables and probably an equally large number of what former Secretary of Defense Donald Rumsfeld would call "unknown unknowns." Nobody in 1911 was predicting the fundamental security challenges of the 20th century: the world wars, the rise of competing totalitarian systems, the superpower rivalries, nuclear deterrence or the rise of China in the context of post-Cold War multipolarity. Even more recently, how many analysts in 1990 would have predicted that two of America's next three

major overseas military operations would involve Iraq and the third would be focused on non-state actors in Afghanistan? To state the matter bluntly, neither I nor anyone else is going to get the details right this time, either. I don't know which countries are going to be the trouble spots of the next century, whether China will prove the next great strategic threat to the West or slowly adopt Western liberalism and its institutions – or both. Merely attempting such prognostications is either for minds greater than my own or for fools aiming to assume positions alongside Mr. Cunliffe-Owen in the annals of great intellectual misfires.

Overview

The most one can reasonably expect in such an exercise is to anticipate one – or maybe a few – of the major challenges the world community will face in the coming decades. In this paper, I mean to focus on a single such problem: the proliferation of technologies that increasingly puts the kind of destructive power traditionally limited to states into the hands of ever-smaller groups. The second half of the 20th century saw a remarkable decline in major state-to-state military conflicts. At first, this was decline caused by nuclear deterrence and the stability imposed by a world dominated by two superpowers and, later, by the combination of a superpower security umbrella, globalization and worldwide economic interdependence. Yet this trend coincided with an augmented ability of relatively small, non-state groups to wage asymmetric conflicts against powerful states. The groups

in question have been growing smaller, more diffuse and looser-knit, while technology has been both facilitating this development and dramatically increasing the ultimate lethality of these groups.

Instead of being futuristic, this latter trend is already well under way across a number of technological platforms, most prominently the life sciences and computer technology. For reasons I shall explain, the trend seems likely to continue and probably even to accelerate. Unlike the technologies associated with nuclear warfare, the technologies now in question were not developed in a classified setting but, rather, in the public domain. They are getting cheaper and proliferating ever more widely for the most noble and innocent of reasons: the desire to cure disease and increase human connectivity, efficiency and capability. As a global community, we are becoming ever more dependent upon these technologies for health, agriculture, communications, jobs, economic growth and development, and even culture. Indeed, the trend is inseparable from – and an inevitable corollary of – a larger trend that is highly salutary: the empowerment of individuals and groups at the expense of governments. The year of the Arab Spring, which has relied heavily on social networking and the distribution of technology to undermine authoritarian governments, is no time for a Luddite aversion to the technologically empowered individual. Nor will it do to primarily view this biotech revolution as threatening since, in reality, it is overwhelmingly positive.

Yet these same technologies – and these same dependencies – make us enormously vulnerable to bad actors with access to them. Whereas only states could formerly contemplate killing huge numbers of civilians with a devastating drug-resistant illness or taking down another country's power grids, these days, every responsible government must contemplate the possibility of ever-smaller groupings of people committing what are traditionally understood as acts of war. Indeed, the latter part of the 20th century and the first few years of the new one saw the migration of the destructive power of states to global non-state actors – most notably al-Qaida. This migration seems likely to continue in the 21st century, ultimately giving every individual with a modest level of education and a certain degree of technical proficiency the power to inflict catastrophic damage. Whereas states once only had to contemplate one another and a select bunch of secessionist militias as strategic threats and could engage with individuals as citizens or subjects, this trend ominously promises to force states to regard individuals as potential strategic threats.

Think of a world composed of billions of people walking around with nuclear weapons in their pockets (Fearon 2003). If that sounds hyperbolic, it's probably only a little bit so. As I shall explain, the current threat landscapes in both the life sciences and the cyber arena are truly terrifying. Both are likely to grow only scarier as the costs of these technologies continue to plummet, as their capacities continue to grow and as the number of people capable of deploying them, either individually or as part of small groups, catastrophically continues to expand. In fact, the more one studies the literature on cyber- and bio-threats, the more puzzling it becomes that a catastrophic attack has not yet happened. And while, based on this lucky past, one becomes tempted to predict that the future cannot be quite that dangerous, the pre-World War I prognosticators offer a caution here too.

In 1913, David Starr Jordan, then-president of Stanford University, scoffed: "What shall we say of the Great War of Europe, ever threatening, ever impending, and which never comes? We shall say that it never will come" (Starr Jordan 1913).

Moreover, in addition to posing menaces on their own terms, bio- and cyber-threats represent a category of threat that presumably will prove broader than these two elements alone. That is, over the coming decades, we are likely to see other areas of technological development that put enormous power – including enormous destructive power – in the hands of individuals. For example, as costs decline and capabilities continue to increase, robotics may prove to be another such area, and nanotechnology as well. There will be others, too – and ones we cannot even imagine today, just as we couldn't imagine the Internet when we first confronted the personal computer. In other words, the broad strategic challenge for global security will not simply be controlling biological terrorism or cyberattacks, which we ought to understand as comparatively well-developed case studies of a larger set of technological challenges. Rather, it will be defining a relationship between the state and individuals with respect to the use and development of such dramatically empowering new technologies that permits the state to protect security while simultaneously insisting that it does so without becoming oppressive.

This challenge clearly poses a major governance question – one without an obvious answer or even an obvious conceptual approach. It seems intuitive that states cannot regard billions of people around the world as potential strategic threats without having that fact fundamentally alter the nature of how those states and individuals interact. Yet the state's initial security instinct here would probably be as ineffective as it would be injurious to human liberty. Whatever the right answer is here, it's certainly not a police state. But if we take that as a given, we are left with vexing questions: Is there an answer? Are we sitting ducks just waiting for one of those people with nuclear weapons in his or her pocket to take them out and destroy the world? Or are there plausible ways to manage the risks of these new categories of technology while reaping their many benefits – and, if so, what might those look like?

In this paper, I do not purport to offer a complete answer to these questions; far from it. I am an expert in neither computer technology nor genetics, synthetic biology or the life sciences more generally. Rather, in what follows, I attempt a discussion of some intellectual strategies for thinking about this governance problem that will almost certainly cut in directions bending current ideological assumptions of both the left and the right. For example, governments' need to understand how bad actors are using these technologies will likely militate against strong forms of privacy protections with respect to their use – both individual privacy protections and corporate privacy and trade-secret protections. Since these technologies developed in the public literature and the relevant materials are all readily available (unlike in the nuclear context, where highly enriched uranium and plutonium are still difficult to come by), the cat really is out of the bag. And, paradoxically, that means that transparency – even radical transparency – in the use and handling of dangerous technologies may offer greater protection against misuse than a more classical non-proliferation approach.

More fundamentally, the diffusion of these technologies will almost certainly precipitate a reduction or erosion of the state's monopoly over security policy. That is, it will distribute responsibility for security to thousands of private-sector actors and potentially millions or billions of individuals whom the technology empowers every bit as much as it does would-be terrorists and criminals. In the cyber context, for example, the communications infrastructure over which attacks will take place is overwhelmingly privately owned and operated. Similarly, in the biotech arena, the best defense against biohazards, whether man-made or naturally occurring, is good public health infrastructure and more of the same basic research that makes biological attacks possible. Most of this research is going on in private companies and universities rather than in government-supported institutions. And, importantly, the biotech industry is not composed of a bunch of defense contractors – or, in other words, people used to being private-sector arms of the state. Increasingly, I shall argue, security will thus take on elements of the distributed application, a term the technology world uses to refer to programs that rely on large numbers of computers all working together to perform tasks that no single system could or would devote adequate resources to.

Indeed, security in this space probably has a great deal to learn from the open-source software movement and the mustering of human capital represented by Wikipedia and other such voluntary collaborations of donated expertise. It is going to have to rely on the idea that there are a great many more good guys than bad guys using these technologies and that, collectively, the good guys can protect their technological platforms more robustly than any top-down security apparatus can. While state power certainly will have a role here – and probably an uncomfortable role involving a lot of intrusive surveillance – it may not be the dominant role that states have formerly played in security.

2 The Decline of State – and the Rise of Personal – Warfare

The 20th century saw both a dramatic rise in state-to-state warfare and an equally dramatic decline in it. The two world wars of the first half of the century gave way to remarkable big-power peace in the second half. This peace had several interlocking causes: There was nuclear deterrence, which prevented the Cold War from ever becoming hot. Later, there was the American security umbrella and globalization, which made the major powers so dependent on one another as to create an exceedingly powerful disincentive to let disagreements and tensions come to blows. It is a remarkable fact – and one probably unprecedented in human history – that a dominant world power (the United States) is today confronting a rising power (China) and that war between them is simply not on the list of options for either party. The latter, after all, holds a trillion dollars of the former's debt, and the former provides the principal market for the latter's manufacturing-based economy. Likewise, even if that were not the case, each side has enough nuclear weapons to keep the other's mind crystal clear. Instead, modern warfare fall into four basic categories: regional conflicts, intrastate conflicts, proxy fights between major powers that will not engage in direct combat, and dramatically asymmetrical wars, such as those between the United States and Iraq or between Russia and Georgia.

This trend of the declining prevalence of big-power warfare seems likely to continue for the same reasons it developed in the first place. Nuclear weapons still provide an enormous disincentive to big-power conflict. Those major powers are growing ever more, rather than less, economically interdependent. For all its warts, the American security umbrella still operates as a major stabilizer for many countries. And institutions like the European Union, NATO and the World Trade Organization are now knitting together countries that once did battle against one another in ways that make large, general conflagrations far less likely.

Yet this trend has not by any means implied an end to warfare, for it has taken place alongside another trend that has pushed in the opposite direction: the increasing ability of non-state groups to wage war in a strategically significant fashion. Non-state actors are, of course, nothing new. In American history, they date back to, well, the American Revolutionary War – and quickly thereafter to Shays' Rebellion and the Whiskey Rebellion. Movie buffs will not forget Spartacus, either. The Palestinian cause has been entirely composed of non-state groupings for decades, and the Israeli cause for the first half of the 20th century was, as well. Indeed, non-state actors have been a feature of the politics of global security for as long as anyone can remember.

That said, they have traditionally been more in the realm of regional irritant than major global factor. The modern international system, generally traced back to the Peace of Westphalia in 1648, has traditionally been "characterized by the coexistence of a multiplicity of states, each sovereign within its territory, equal to one another, and free from any external earthly authority" (Gross 1948: 28–29). National security policy has largely been formulated within this Westphalian rubric, with state control over the exercise of military force as one of the distinctive features of the modern era (Krasner 1999: 20).[1]

By the time of the Treaty of Westphalia, writes another scholar, "[w]ar had become a matter between sovereigns only, and for a legally recognized armed conflict to exist there had to be a hostile contention by means of armed forces carried on between states" (Green 2008: 35). Israeli historian Martin van Crevel has described this model of armed conflict as "trinitarian warfare": "It is the government that directs, the army that fights, and the people who watch, pay, and suffer" (Creveld 1993: 20). This state-centric model of warfare assumes that sovereign institutions have a monopoly on violence. That assumption, while never perfect, described the broad architecture of international security for hundreds of years. To take one example, the Whiskey Rebellion was a problem for George Washington, but it wasn't a problem for international security.

But that is changing. Today, non-state actors – from terrorist groups to organized crime syndicates – play a growing role in the basic architecture of international affairs. The ease of international travel, the fluid flow of information, transnational corporations and the broader panoply of phenomena that go under the rubric of "globalization" have posed challenges to the concept of territorial sovereignty. And the groups that are posi-

1 Krasner (1999: 20) describes the Westphalian model as "an institutional arrangement for organizing political life that is based on two principles: territoriality and the exclusion of external actors from domestic authority structures."

tioned to exploit this, and that potentially wield the power to wage war, are growing ever smaller. Today, with the presumably brief exception of America's involvement in Libya, the United States is involved in no wars against states but, rather, only conflicts with non-state groupings. Nevertheless, over time, merely managing these conflicts has cost hundreds of billions of dollars and required forces numbering in the hundreds of thousands.

These developments greatly blur the conceptual and legal framework within which we have traditionally constructed international relations and national security policy. The distinction between foreign and domestic threats – once glaring and obvious – has become more tenuous. And, as a result, the roles of domestic law enforcement aimed at civilians, military actions aimed at foreign enemies, and intelligence actions aimed at foreign military or civilian targets tend to collapse, as well.

The September 11 attacks were perhaps the most startling harbingers of this new, post-Westphalian world. But they were not the only ones – and they almost surely will not be the last. Al-Qaida became possible as a result of a variety of factors endemic to modern life. One is the mobility of money and people, as well as the ease of communication in the modern world. Another is technology and the cycles we go through: First, we are excited about them, then we exploit them, and then we become dependent on them – but with an insufficient appreciation of the degree of vulnerability this dependence generates. Former Department of Homeland Security policy chief Stewart Baker makes this point elegantly: "Technology – cheap commercial jet travel – made the attacks possible. In fact, it made attacks like September 11 more or less inevitable" (Baker 2010: 12). We build airplanes and fly them all over the world. We dramatically lower the price of commercial air travel until long-distance travel is a norm for people's day-to-day lives. And nobody spends much time considering the possibility that someone smart and creative can make missiles out of our commercial jets using nothing but box cutters and ruthlessness. The more dependent we become on universally available technologies, the more we make ourselves vulnerable to the devastating misuse of those technologies. This is not a Luddite argument against technological development; rather, it is an argument against blindly enthusiastic dependence on broadly disseminated technologies that give awesome power to anyone who knows how to use them.

Critically, the privatization of violence does not stop with groups like al-Qaida, which is really just one of many points along a spectrum of decreasing public authority and increasing non-state threats. These points begin with state-sponsored terrorist groups and also include groups like al-Qaida (which was both state-sponsored and state-sponsoring) as well as groups vying for the takeover of failed states. They extend down through private international organizations, major organized criminal groupings, gangs, millenarian sects and, in principle, all the way down to individuals. After all, as the FBI finally concluded, it was an individual, rather than a group, who launched the 2001 anthrax attacks.

When such small groups only had guns, their lethality was limited. But modern communications technology has increased it dramatically. What's more, technologies that offer opportunities for extreme destructiveness up the ante even further. As John Robb has compellingly put it: "The threshold necessary for small groups to conduct warfare has finally been breached, and we are only starting to feel its effects. Over time, perhaps in as

little as twenty years, and as the leverage provided by technology increases, this threshold will finally reach its culmination – *with the ability of one man to declare war on the world and win*" (emphasis in original) (Robb 2007: 8).

These technologies – of which biotechnology and globally networked computers are the paradigmatic examples – have certain common characteristics that bear emphasis. First, they are widely disseminated technologies that depend on readily available training and materials. Unlike nuclear technologies, they did not develop principally in classified settings, such as in government-run labs and with the government controlling access to the key materials. Rather, they developed in public, in open dialogue and with non-military purposes in mind. Indeed, we didn't sequence the human genome in order to figure out how to design viruses to kill people. We didn't build the Internet so that terrorists could seize control of the Hoover Dam – or even so that our intelligence agencies could seize control of some other country's dams. Yet a publicly accessible literature now exists to teach bad guys how to do horrific things – and, unlike highly enriched uranium, the materials are neither scarce nor expensive.

Second, the destructive technologies are virtually inseparable from the socially beneficial technologies that give rise to them. The research on how to use genetics to cure and prevent disease is the same research that, in the wrong hands, can be used to cause disease. A paper on how to shield computers against viruses necessarily involves analysis of viruses that one can use to write stronger ones. There is no way to do defensive research without potentially empowering the bad guys, as well.

Third, the use of these technologies blurs the distinction between foreign and domestic threats and, indeed, makes attribution of any attack extremely difficult. As every student in a biological laboratory and every individual on his home computer becomes a possible threat to national security, traditional techniques of surveillance, deterrence and non-proliferation become increasingly ill-suited to detecting and preventing terrorist activity. Large numbers of cyberattacks already take place, with attribution impossible or long delayed. In the case of the anthrax attacks, attribution took seven years and remains contested to this day. Indeed, as often happens in these cases, a target state will not be able to determine whether its attacker is another state, a political group, a criminal group or a lone gunman.

3 The Bioterrorism Threat

The life sciences present perhaps the prototypical case of this type of technological development, realistically threatening to put the power of a WMD attack in the hands of, if not the average person, certainly many above-average people with relatively inexpensive equipment and basic training in genetic engineering. Biological weapons are unique among weapons of mass destruction in that, like nuclear weapons, they have the capacity to inflict truly catastrophic damage, yet, like chemical weapons, they are comparatively inexpensive and easy to produce. The technology required for their production is generally the same as the technology used in legitimate life-sciences research; indeed, it is the

bread-and-butter stuff of the biotech revolution that has done so much good throughout the world. Precisely because modern biotechnology has so much promise and offers so many benefits in so many walks of life, the materials and skills required to develop these weapons are not rare. So, while it may be difficult for even a highly trained individual to build his or her own nuclear weapon, an individual with relatively modest expertise and resources could potentially obtain or develop his or her own biological weapon with global consequences. As costs continue to fall, the number of people whom governments around the world have to regard – at least in theory – as being capable of having their own personal WMD program grows commensurately.

This is happening fast. Princeton bioterrorism expert Christopher Chyba has likened the proliferation of gene-synthesis capability to the explosion in computer technology known as Moore's Law. Named after Intel Corporation founder Gordon Moore, Moore's Law observed in 1965 that the processing speed and memory of computers double every 18 months – a trend that has remained true ever since. Chyba states that "[j]ust as Moore's law led to a transition in computing from extremely expensive industrial-scale machines to laptops, iPods, and microprocessors in toys, cars, and home appliances, so is biotechnological innovation moving us to a world where manipulations or synthesis of DNA will be increasingly available to small groups of the technically competent or even individual users, should they choose to make use of it" (Chyba 2006: 12).

Chyba notes that the cost of synthesizing a human genome could soon be as low as $1,000 and that, along with cost decreases, the efficiency of biotechnology continues to increase (Nouri and Chyba 2009: 234). According to one calculation, the speed of DNA synthesis increased 500 times between 1990 and 2000 (Chyba 2006: 12). Another expert had calculated that, by 2010, an individual working alone would be able to synthesize genetic materials 100 times faster than he could in 2003 (Rabodzey 2003: 3). To give a sense of what this means for a person's ability to build his or her own WMD arsenal, while it took researchers at the State University of New York three years to synthesize the complete polio virus in 2002, the following year, a different group of researchers synthesized a viral genome of comparative length in only two weeks (Chyba 2006: 12).

Furthermore, biological weapons do not work like other weapons of mass destruction. The long incubation periods for many pathogens mean that an infected individual can travel and infect others before contamination becomes apparent, thereby making it difficult to limit the impact of an attack. Moreover, illnesses caused by biological weapons are often hard to distinguish from naturally occurring outbreaks. For example, it took investigators a year to realize that a 1984 salmonella outbreak in Oregon was the result of an attack by disciples of the Indian guru Bhagwan Shree Rajneesh (Chyba 2002: 129). Unless the culprits publicly acknowledge their responsibility, this can accentuate the attribution problem discussed above. The difficulty of attribution, combined with the fact that authorities may not learn of an attack until symptoms emerge days or weeks after infection, blunts the effectiveness of traditional models of deterrence and response.

The converse risk also applies: Authorities may wrongly attribute a natural outbreak to an act of terrorism. Although investigators eventually concluded, for example, that the 1999 outbreak of West Nile encephalitis in New York was the result of natural causes, it

had several of the hallmarks of a terrorist attack. The disease had never occurred in the Western Hemisphere and, just months before the outbreak, an Iraqi defector had claimed that Saddam Hussein was developing the West Nile virus into a biological weapon (Chyba 2001: 96–97). The potential for such mistakes can undermine a government's credibility, further exacerbating the destabilizing effects of a terrorist attack.

What's more, deadly pathogens are not that hard to come by, and many occur naturally. Indeed, some of the most notable and terrifying pathogens that occur naturally include anthrax, the bubonic plague and viral hemorrhagic fevers, such as tularemia and the Ebola, Marburg and Venezuelan equine encephalitis viruses. The fact that these can be collected in the natural environment was not lost on the notorious Japanese cult Aum Shinrikyo, which tried to obtain Ebola strains in Zaire. In addition, many pathogens are stockpiled by commercial companies for legitimate purposes, although controls on these stockpiles have tightened in recent years.

And then there's the fact that even pathogens like smallpox and the 1918 flu virus, which have been wiped out in the wild, can now be recreated. The fact that literature describing – and even routinizing – genetic-engineering projects that involve the creation, modification and enhancement of deadly pathogens is available in the public domain should be at least as terrifying to policymakers around the world as box cutters or guns on airplanes. What's more, viral genomes are relatively small. Many have already been mapped, and the materials required to synthesize them or adapt them from related pathogens are all commercially available. Likewise, scientists have repeatedly demonstrated that, if terrorists – or individual bad guys – have the will, science has a way:

- In 2001, Australian researchers published the results of a study in which they used gene-splicing technology to create a mousepox virus impervious to vaccination (Jackson et al. 2001). (Mousepox is a virus closely related to human smallpox, although it does not cause disease in humans.)
- In 2001, a team of virologists in Germany and France constructed Ebola virus from three strands of complementary DNA (Volchkov et al. 2001).
- In 2002, researchers from the State University of New York, Stony Brook, published studies of de novo DNA synthesis of the polio virus, which they had constructed using nucleotide fragments purchased from a mail-order biotechnology company (Cello, Paul and Willmer 2002).
- In similar studies, scientists have successfully synthesized the 1918 Spanish influenza virus (Tumpey et al. 2005), which infected an estimated one-third of the world's population and killed between 50 and 100 million people worldwide (Taubenberger and Morens 2006), as well as the Encephalomyocarditis virus, which can cause fatal febrile illness in humans (Svitkin and Sonenberg 2003).

To be sure, terrorist groups and individuals still face technological obstacles to launching a global pandemic, but they are growing ever more surmountable. As technology continues to improve, the synthetic creation or adaptation of larger, more complex pathogens – including, potentially, the smallpox virus (Rabodzey 2003) – will become cheaper and easier for a wider array of potential bad actors.

If recent history is any guide, that's an ominous possibility. For while no terrorist group has thus far successfully launched a mass-casualty biological attack, a range of cases demonstrate that there is no dearth of people who would like to do so. For example, in the early 1990s, the Aum Shinrikyo cult expended great effort in its attempts to obtain biological weapons. Before killing 12 people and injuring more than 5,000 by releasing sarin nerve gas on a Tokyo subway in 1995, cult members attempted to release botulinum toxin in Japan's parliament, sent a mission to Zaire to obtain strains of the Ebola virus and released anthrax spores from atop a building in Tokyo (Kellman 2001: 425).

The case of Larry Wayne Harris provides another chilling example of a non-state actor's potential bioterrorism capabilities. Harris was a member of the Aryan Nations who easily obtained the bacterial agent of the bubonic plague from a private company using the stationery of a fictitious laboratory. After the company shipped the bacterial cultures to his home, an employee became concerned and contacted the Centers for Disease Control and Prevention (CDC). Thus alerted, the authorities obtained a search warrant and discovered biological pathogens, as well as explosives, in Harris' car and home. Harris explained that he was stockpiling weapons in preparation for an imminent Armageddon (ibid.: 449–50).

And, of course, the threat of bioterrorism became a reality with the anthrax attacks in October 2001. Just weeks after the devastating attacks of September 11, 2001, someone mailed anthrax-contaminated powder from a mailbox in Princeton, New Jersey, killing five people, injuring 17, shutting down mail services and resulting in the evacuation of federal buildings, including Senate offices and the Supreme Court. Although the Justice Department closed its investigation in 2008 after the prime suspect, a bio-defense employee named Bruce E. Ivins, committed suicide, doubts still linger about the case (Shane 2008; Warrick, Thompson and Davis 2008). In any event, the fact that it took investigators seven years to develop an indictable case against a single individual illustrates the security and law-enforcement challenges posed by even a relatively low-impact bioterrorism event.

If a terrorist were to overcome the challenges inherent in developing a naturally occurring pathogen into a deployable weapon, the consequences could be devastating. For example, the U.S. Office of Technology Assessment has estimated that an airplane flying over a densely populated area, such as Washington, D.C., could kill as many as 3 million people with 100 kilograms of properly aerosolized anthrax (U.S. Office of Technology Assessment 1993: 53–54). A contagious virus specifically engineered for lethality against a relatively unimmunized population could, at least theoretically, be even worse. In the world of low-probability, high-impact events, this type of attack stands out for its relative plausibility.

4 The Cyber Threat

The threat of cyberterrorism – and the vulnerability of the world's network infrastructure, more generally – similarly illustrates the growing capacity of small groups to become players in international relations and global security issues. As is the case with biotechnology,

the information technology underlying today's computer and communications networks is inherently a dual-use technology. Military IT depends largely on commercial IT developed in the private sector (Owens, Dam and Lin 2009: 2.2.1). According to one estimate, 95 percent of the U.S. military's information transfers occur on civilian networks (Antolin-Jenkins 2005: 133). Likewise, the expertise needed to launch cyberattacks is widely distributed throughout the world. A cyberattack could aim at a nation's military operations or seek to disrupt its social and economic activity. Such an attack could come from a rival nation (presumably on a smaller scale) or from the laptops of members of criminal gangs, politically motivated hacking groups or simply disaffected individuals. And, as with the anthrax attacks, identifying the perpetrator involves both time and, ultimately, significant doubt. Indeed, the anonymity and accessibility of the Internet make deterring and attributing cyberattacks particularly difficult.

Globalized IT systems, moreover, are by their very nature borderless, thus enhancing the ability of terrorists, organized criminals or rogue individuals to inflict damage from wherever they happen to be in the world. In this sense, too, the problem shows considerable similarity to bioterrorism and similarly challenges the principle of territoriality on which the current international order is based. In short, like biological attacks, cyberterrorism conflates the realms of national security and criminal law enforcement while, at the same time, blurring the distinction between domestic and international authority.

The possible objectives of a cyberattack vary as widely as do the societal functions that now depend on computerized networks. Most attacks involve garden-variety attempts at fraud and theft. On a grander scale, they can also involve espionage. Owens, Dam and Lin (2009: 2.3.2) also provide a number of other possible objectives: An attack could delete the data stored at power-generation facilities, thereby shutting down a country's energy–production infrastructure. An attack on a network used by the military to plan for its operations could alter the order in which food supplies and equipment are delivered during an operation. An attacker could infiltrate a network and pose as a member of a government agency in order to issue fake orders or spread disinformation. Or an attacker could conduct a "denial-of-service" attack, which degrades a network by shutting down its operations or flooding it with traffic.

Unlike with bioterrorism, one does not have to speculate to imagine individuals, small groups or even governments exploiting contemporary vulnerabilities in computer security. In fact, this has become an everyday occurrence. Computer crime, identity theft and so-called "cyber-exploitation" (i.e., stealing large quantities of supposedly protected information from computer systems) is big business and as routine a part of Internet life as street crime and house break-ins are a part of life in big cities. Indeed, a National Science Foundation report from 2006 stated that "nearly all indicators of frequency, impact, scope, and cost of cybersecurity incidents show a continuously worsening picture. This is true whether one considers the losses due to IT-based fraud and theft, identity theft and attacks on personal information, incidence of viruses and malicious code, number of compromised systems, or other types of impact" (Goodman and Lin 2007: 32).

In addition, at the more dangerous end of the scale, the relatively low cost and accessibility of computer technology make it uniquely well-suited for asymmetric attacks by

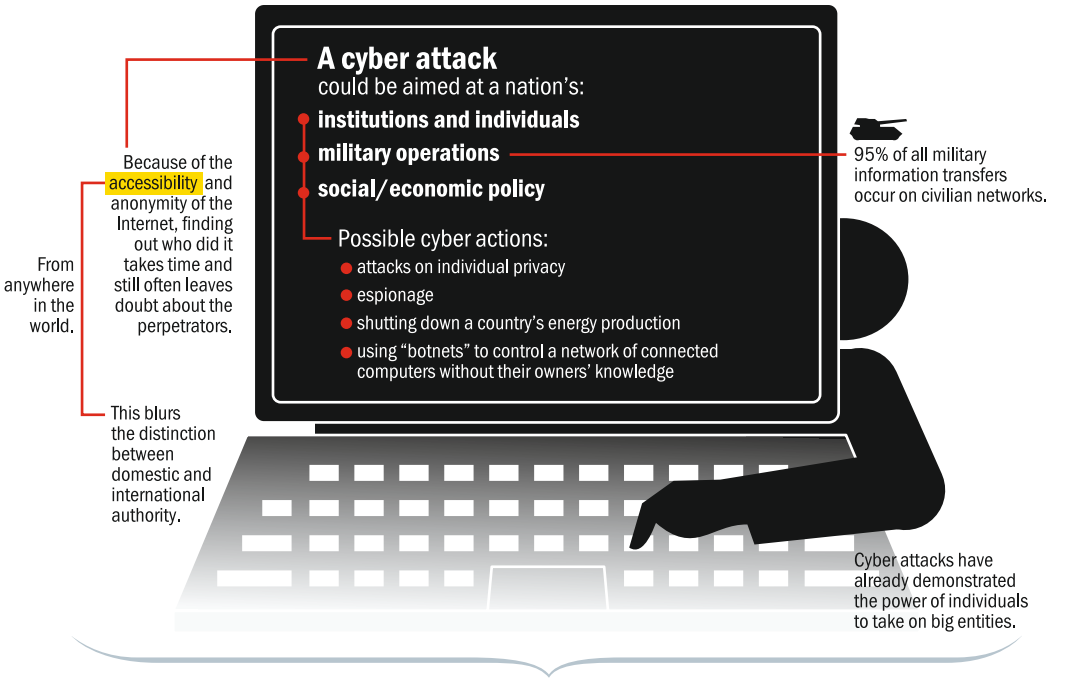
small groups or individuals – and even for teenagers looking to pull off sophisticated pranks. For example, in 1998, two California teenagers and a third hacker in Israel, with no apparent terroristic intent, penetrated Pentagon computers in an attack serious enough for the Pentagon to initially notify then-President Clinton that it was probably coming from Iraq (Graham 1998). In 2000, a Canadian boy shut down several major websites, including CNN.com, Amazon.com, and Yahoo.com (Brown 2001). In 2004, a teenager in Germany admitted to having created the Sasser and Netsky Internet worms, which forced airlines to ground or delay flights and had British coastguard stations working with pen and paper (Tieman 2004). And, of course, groups of hackers – most notably, the collective known as Anonymous – have famously launched distributed attacks in recent months on a range of targets ranging from Sony to companies that refused to host WikiLeaks. Indeed, cyberattacks already demonstrate the power of individuals to – for whatever reason – take on very big entities.

What's more, a number of high-profile incidents in recent years have underscored the fact that cyberwarfare itself is no longer in the realm of science fiction. For example, in 2003, a "worm" infected a closed nuclear power plant in Ohio and disrupted its computer systems for five hours (Wilson 2003). In 2007, the Department of Homeland Security conducted a test in which it hacked into the control system of a model power plant and destroyed a generator by changing its operating cycle (Meserve 2007). The CIA later revealed that real cyberattacks have been conducted on foreign power plants by people seeking ransoms (Bridis 2008). And, of course, the possibility of cyberwarfare involving real nuclear power plants was vividly on display in the case of the so-called Stuxnet worm, which attacked the Iranian uranium-enrichment program in 2010 by speeding up specific models of enrichment centrifuges.

Global networks also have potent applications in espionage. In a series of attacks known as "Titan Rain," unknown hackers using computers in China copied sensitive information from the U.S. Defense Information Systems Agency (DISA), the U.S. Army's Redstone Arsenal in Alabama, the Army Space and Strategic Defense Installation, and several computer systems used by U.S. government contractors (Lewis 2005). Particularly worrisome was the fact that the attacks went unnoticed for several months. In another illustration of the attribution problem, Pentagon officials suspected that the Chinese government was behind the attacks, although this was never proven (Graham 2005).

Then there were the cyberattacks in Estonia in 2007 and Georgia in 2008. Several days after a diplomatic row erupted between Russia and Estonia over the latter's relocation of a monument dedicated to the Red Army, the computer networks of Estonia's banks, media outlets and government agencies were crippled by a flood of bogus requests for information. The attackers used a program known as a "botnet" (short for "robotic network"), which controlled a massive group of interconnected computers, to simultaneously bombard Estonia's networks. James A. Lewis, a security expert at the Center for Strategic and International Studies, explains that the perpetrators of the attack most likely took control of computers without the knowledge of their owners and used the hijacked machines to remotely send the deluge of messages (Lewis 2007). Although Estonia openly accused Russia of cyberwarfare, the culprits were never found.

The cyber threat



Is this warfare?
Are members of alliances (such as NATO) obliged to respond if one of their members is attacked?
How? And to whom?

Two key areas of concern

More and more, we depend on these technologies.

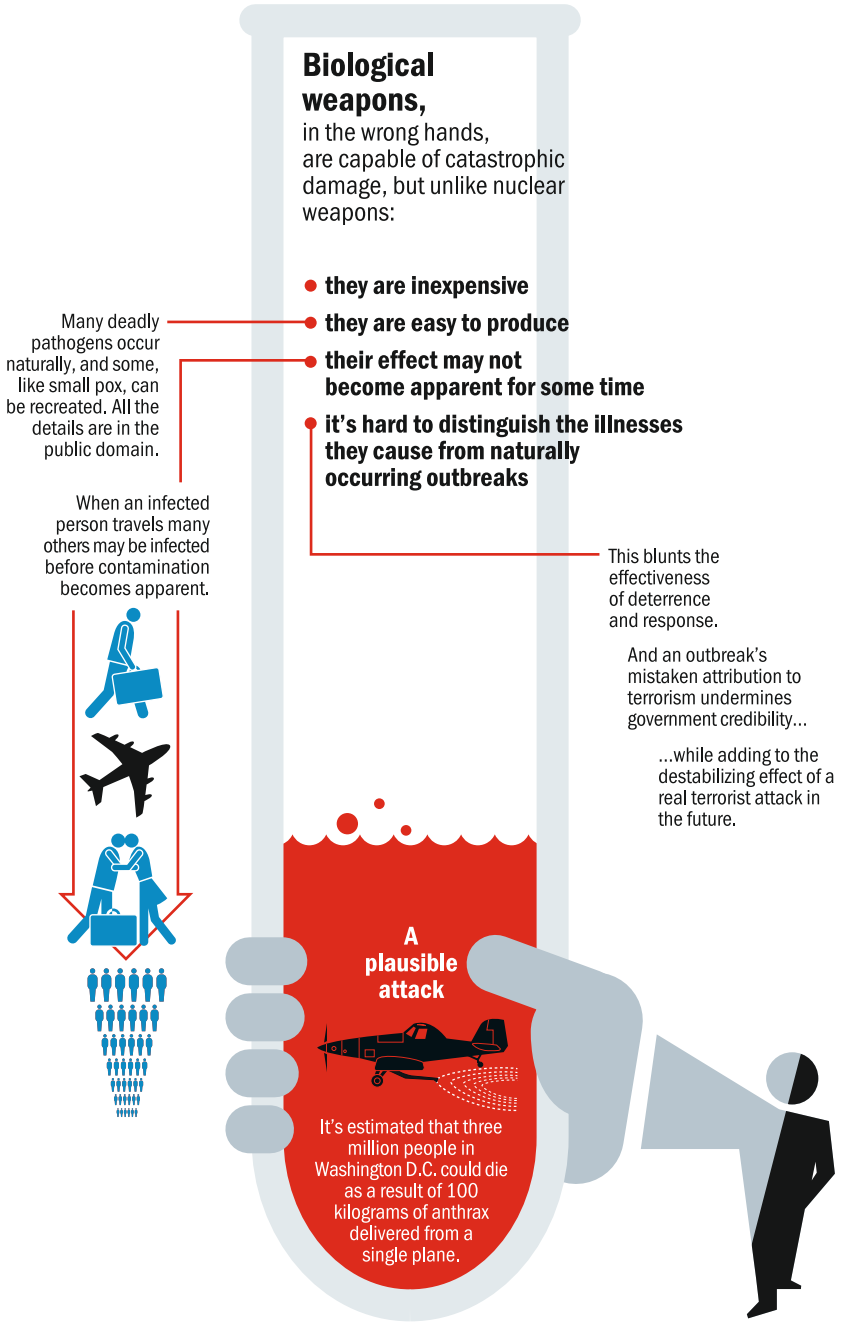
This trend is inseparable from a global movement to empower **individuals.** And that is good.

But there is dark side to this. The more we depend on these new technologies, the more vulnerable we are to **other individuals** who can use them with devastating results.

The problem

Socially beneficial uses of new technologies and destructive uses of the same technologies are linked: the research used to cure disease is the same research used to cause disease.

The bioterrorism threat

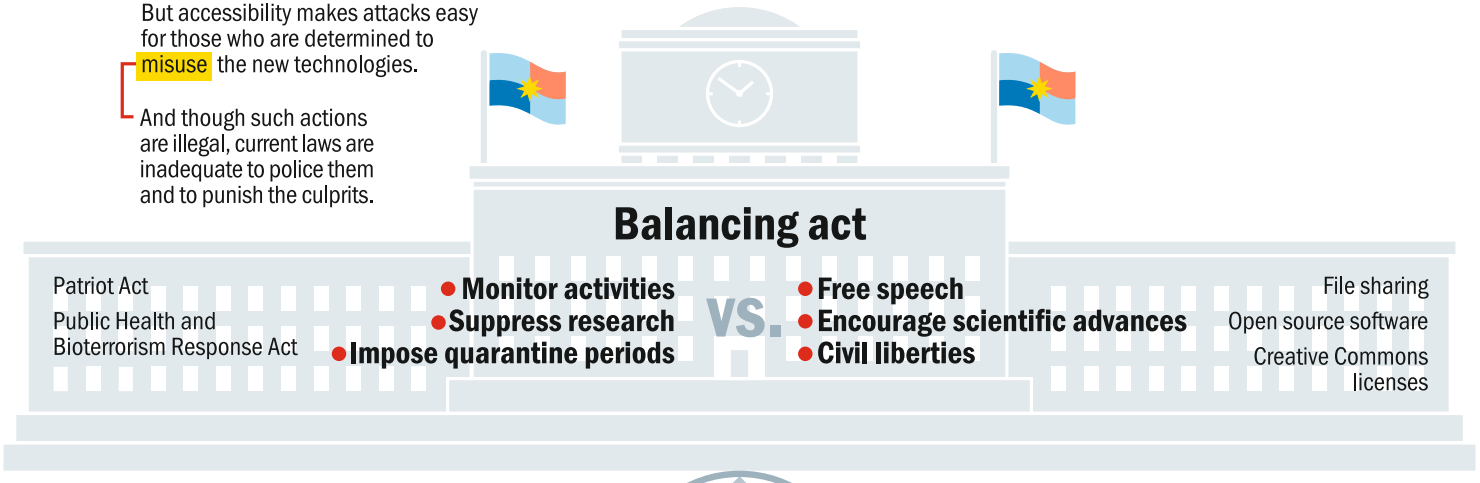


The current state of governance

- **Advances in biotech and the Internet are salutary.**
- **Both depend on open access.**

But accessibility makes attacks easy for those who are determined to misuse the new technologies.

And though such actions are illegal, current laws are inadequate to police them and to punish the culprits.



But,

because the rapid development in the biotech and cyber arenas has largely taken place in private, not government, hands, the basic presumption that security is now a government function is questioned. **The government no longer controls the channels through which bio- and cyberattacks can occur.**

The power of the individual

"Perhaps in as little as 20 years ... one man [will have the ability] to declare war on the world and win."—John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization*

"Think of a world composed of billions of people walking around with nuclear weapons in their pockets."—James Fearon, *Catastrophic Terrorism and Civil Liberties in the Short and Long Run*

The attacks in Estonia raised a number of puzzling questions about the status of cyberattacks in international law, such as: What constitutes an "armed attack"? Is "warfare" to be defined by the methods used, the effects or the intent of the attacker? Was NATO, of which Estonia is a member and whose members regard an attack against one member state as an attack on all member states, obliged to respond? And, if so, against whom? (Applebaum 2007) The following year, when Russia and Georgia fought a brief war over two breakaway Georgian provinces, Russian hackers crippled Georgia's communications and banking systems with a series of attacks that successfully resisted all Georgian countermeasures.[2]

The past few years have seen exceptionally high-profile cybersecurity failures. After the Dalai Lama found his computer systems hacked in 2008, he hired a computer-security team to investigate. They found a highly sophisticated set of attacks out of China directed not merely at the Dalai Lama, but also at Indian embassies around the world, various other Asian governments, the Associated Press, Deloitte & Touche and NATO. In 2010, Google announced that it had been hit with similar attacks, as had numerous other businesses (Baker 210: 209–213). Likewise, the Iranian nuclear program fell victim to the

2 For a good summary of the Estonian and Georgian attacks, see Chapter 1 of Clarke and Knake 2010.

Stuxnet attacks, which are widely believed – though not acknowledged – to have been either an Israeli, American or joint Israeli-American operation.

As with biological attacks, it is hard to assess the probability of a truly catastrophic cyberattack, but it is certainly not negligible. In 2006, the National Science Foundation wrote that "high-level threats – spawned by motivated, sophisticated, and well-resourced adversaries – could increase very quickly on a very short time-scale, potentially leading to what some dub a 'digital Pearl Harbor' (that is, a catastrophic event whose occurrence can be unambiguously traced to flaws in cybersecurity) – and that the nation's IT vendors and users (both individual and corporate) would have to respond very quickly when such threats emerge" (Goodman and Lin 2007: 49). Similarly, former Director of National Intelligence Admiral Michael McConnell has repeatedly warned of an electronic Pearl Harbor potentially involving the financial sector. Such an attack is probably still the province of state-level operations, however, and we can hope that defensive improvements to computer systems belonging to critical infrastructure will keep the truly devastating cyberattack out of the individual's reach.

What are not the province of states even now are the low- to medium-grade attacks on a widespread scale. Indeed, there is a continuum here between entirely legitimate cyber-organizing, which can often serve to erode government power in salutary ways, cyber-harassment and "hacktivism," and full-on attacks. At one end of this spectrum is the sort of social-media organizing that has played such a key role in the Arab Spring. In the intermediate space are actors, such as WikiLeaks and Anonymous, that aggregate the products of empowered computer use by entire communities of politically energized actors in a way that facilitates the disruption and exposure of both governmental and private entities. At the other end of the spectrum are out-and-out cyber-intrusion, -exploitation and -attacks. What all have in common is the use of widely distributed networked computer architecture to allow individuals – for good or ill – to engage in conflict against governments.

5 The Current State of Governance

It rather understates the matter to say that current governance of both the cyber- and bio-threat arenas is hopelessly inadequate to the task of preventing the disasters one might reasonably anticipate. This is not chiefly a function of the fact that generating governance changes that carry real costs in the absence of dramatic precipitating events is always difficult – though that also plays a role. It also reflects the fact that, in both cases, the ideal governance approach is far from obvious and nobody quite knows how to attack the problem. Even if one could stuff the cat back in the bag here, so to speak, who would want to? After all, the Internet is a wonderful thing – as is the biotech revolution. Both pervasively depend on precisely the open culture that has created the vulnerabilities I have been describing. And doing bad things with these technologies is generally illegal already. The problem is not that we don't have laws prohibiting the abuse of these technologies. Rather, it's that the laws do not – and probably cannot – effectively address the

attribution problems in play with both technologies, nor can it easily offer much in the way of prevention.

Once again, the life sciences offer a vivid case in point. Over the past decade, the relevant laws have developed rather admirably, and it's now hard to imagine anyone doing anything horrible without running afoul of them. At the same time, it's also hard to imagine the current laws doing much more than inconveniencing someone committed to developing or releasing a biological agent that could do great damage.

Traditionally, states treated biothreats either as naturally occurring phenomena viewed through the lens of public health policy or as state-to-state weapons-proliferation problems. For example, the 1972 Biological Weapons Convention ("BWC"), ratified by the United States in 1975, saw the problem of biological weapons almost entirely in terms of states and official biological-warfare programs – a function of the fact that, back then, it really was science fiction to imagine anyone but a state developing or using significant biological weapons. Article I of the BWC prohibits signatory nations from developing, producing or stockpiling "[m]icrobial or other biological agents ... that have no justification for prophylactic, protective or other peaceful purposes" (BWC 1972). The restrictions of the BWC in the United States did not apply to private individuals until the passage of the Biological Weapons Anti-Terrorism Act of 1989 (BWATA), which criminalized the production, possession and transfer of biological agents "for use as a weapon" (BWATA 1990).

Despite these measures, the risks of bioterrorism posed by private groups and individuals continued to go largely unnoticed until 1995, when Larry Wayne Harris demonstrated the seriousness of the threat. This episode, described above, spurred lawmakers to tighten controls on the transfer of dangerous biological materials. As part of the omnibus Anti-Terrorism and Effective Death Penalty Act of 1996 (AEDPA), Congress restricted access to biological materials and required the Secretary of Health and Human Services to implement regulations restricting the transfer of particularly dangerous "select agents" (AEDPA 1996). As part of its new authority, the CDC required that labs handling select agents be registered and required that they only transfer such agents to other registered labs.

Congress next stepped into the fray following the September 11 attacks and the fatal anthrax mailings following shortly thereafter by passing two pieces of additional legislation. First, the Patriot Act strengthened the biological weapons statute to make it a crime to possess "any biological agent, toxin, or delivery system of a type or in a quantity that ... is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose" (U.S.A. Patriot Act 2001). The Patriot Act also prohibited the possession of certain listed biological agents by a "restricted person" or their transfer to such a person.[3]

3 *Biological Weapons Act,* § 175b(a)(1), (d)(2). The law defined "restricted person" to include anyone who:
(A) is under indictment for a crime punishable by imprisonment for a term exceeding 1 year;
(B) has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year;
(C) is a fugitive from justice;

Second, Congress passed the Public Health Security and Bioterrorism Preparedness Response Act (PHSBPRA), also known as the Bioterrorism Act, to enhance monitoring of the possession and transfer of select biological agents. The new law added a series of factors for the Department of Health and Human Services to consider in listing select agents and required facilities registering to handle them to provide "information regarding the characterization of listed agents and toxins to facilitate their identification, including their source." It further required the department to "maintain a national database that includes the names and locations of registered persons, the listed agents and toxins such persons are possessing, using, or transferring, and information regarding the characterization of such agents and toxins" (PHSBPRA 2002).

One of the most important – and most controversial – of the Bioterrorism Act's sections provided for a rudimentary background check for people registering to handle select agents to make sure they were not restricted persons prohibited from doing so. This effectively authorized the FBI to require anyone seeking access to listed biological agents to submit to a "security risk assessment." The FBI regulations implementing this provision permit the FBI to share an applicant's information with other governmental agencies, including law-enforcement and private organizations (FBI n.d.). Some in the scientific community have expressed concern that the provisions related to the security risk assessment discourage qualified individuals from engaging in legitimate biological and agricultural research "because of the apparent infringement of these rules on individual liberties under the Fourth Amendment" (National Research Council 2004: 44).

While the government's response to bioterrorism to date has largely focused on enhancing the monitoring and control of biological research and materials, the continuing threat has also prompted calls for extending regulatory authorities both to suppress research and to respond to biological attacks. On the prevention side, proposals to restrict the flow of information – including controls on the publication of research papers, scientific conferences and the sharing of information with foreign scientists – have raised serious concerns about the implications of bioterrorism policy for free speech and scientific advancement (ibid.). Meanwhile, proposals to increase the government's response capabilities – in particular, proposals to broaden federal and state power to detain and quarantine those who may have been infected by an attack – have threatened to stress traditional norms of due process.

(D) is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802));
(E) is an alien illegally or unlawfully in the United States;
(F) has been adjudicated as a mental defective or has been committed to any mental institution;
(G) is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country as to which the Secretary of State, pursuant to section 6(j) of the Export Administration Act of 1979 (50 U.S.C. App. 2405(j)), section 620A of chapter 1 of part M of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), or section 40(d) of chapter 3 of the Arms Export Control Act (22 U.S.C. 2780(d)), has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism; or
(H) has been discharged from the Armed Services of the United States under dishonorable conditions.

The CDC has also recommended that states enhance their isolation and quarantine authorities in order to respond to attacks employing biological weapons. At the CDC's request, the Center for Law and the Public's Health, a joint venture of Georgetown University and Johns Hopkins University, drafted the Model State Emergency Health Powers Act, which grants state officials a number of coercive powers in the event of a declared public health emergency (Gostin et al. 2002: 622).

In 2005, the CDC proposed expanding its isolation and quarantine powers to permit the "provisional quarantine," for a period of three business days, of someone suspected of having a listed communicable disease (CDC 2005). This proposal would have allowed the detention of anyone suspected of having such a disease so that officials could medically determine whether that person was in fact a carrier. When proposed, these regulations drew considerable criticism from civil libertarians concerned about the constitutional implications of such a broad detention power. In 2009, the Obama administration showed signs of renewed interest in the idea, though it has yet to move forward with its implementation (Gerstein 2009).

The biotech industry is also beginning efforts at self-regulation. Gene-synthesis companies that sell sequences of genetic material prepared to order have begun screening orders for sequences that match – or match significant fragments of – pathogens listed as select agents (Bügl et al. 2007; Minshull and Wagner 2009). Some have proposed going further and actually building such screening mechanisms into available gene-synthesis equipment (Nouri and Chyba 2009).

In short, it's hard to imagine that someone could build a personal WMD arsenal without running afoul of numerous criminal laws and regulatory regimes, and various systems are either in place or being developed to flag bad actors before they strike. That said, it's almost equally hard to imagine any of this deterring someone truly committed to launching a devastating attack, particularly if such a person lives or operates abroad. Indeed, it's hard to imagine these laws, regulations and systems doing more than putting a series of ultimately surmountable roadblocks in such a person's way.

On the surface, the governance picture seems marginally less grim with respect to cyberattacks, since the United States has a well-developed body of criminal law prohibiting computer intrusions – and a body of law with a considerable history of enforcement. Indeed, prosecutions for cybercrimes are relatively routine. The federal criminal code has statutes including broad prohibitions against computer fraud and unauthorized access to computer systems (e.g., 18 U.S. Code Sec. 1029, prohibiting "fraud and related activity in connection with access devices" and 18 U.S. Code Sec. 1030, prohibiting "fraud and related activity in connection with computers"). It also prohibits the unauthorized interception "of wire, oral, or electronic communications," (e.g., 18 U.S. Code Sec. 1362, prohibiting "malicious mischief" with regards to "communications lines, stations or systems") as well as that of stored communications, and it further prohibits unauthorized disclosures of such stored communications and certain transactional records to third parties (e.g., 18 U.S. Code Sec. 2701, prohibiting "unlawful access to stored communications," and 18 U.S. Code Sec. 2702, prohibiting "voluntary disclosure of customer communications or records"). Other federal laws prohibit the private use of devices to record communications

addressing information (e.g., 18 U.S. Code Sec. 3121, prohibiting "pen register and trap and trace device use"). Likewise, more general criminal prohibitions – such as the Economic Espionage Act of 1996 (18 U.S. Code 1831–1839, prohibiting "economic espionage" and "theft of state secrets" with related exceptions, procedural rules, international jurisdiction and definitions) – have applications in the cyber context, as well.

What's more, the international law environment for the regulation of cyberattacks looks superficially better than the comparable one for biological weapons. Unlike the BWC, with its residual focus on state-level weapons programs, the Council of Europe's Convention on Cybercrime chiefly focuses on individual and group activity, requiring all member states to develop a "common criminal policy aimed at the protection of society against cybercrime." The convention obligates states to pass laws prohibiting illegal access to computer systems, the illegal interception of communications, interference with data and systems, and the misuse of electronic devices. Likewise, it further obligates states to cooperate with one another's law-enforcement efforts, including by extraditing suspects wanted in other signatory states (Council of Europe 2001).

Unfortunately, the apparently strong development of useful law in this arena is something of a mirage. The Convention on Cybercrime has only 47 signatory states, of which only 31 (including the United States) have actually ratified it. These do not include Russia and China, two cyberattack powerhouses, or India, where a great deal of software is written (Council of Europe n.d.). Indeed, when it comes to cyberattacks, much of the world is still the Wild West – particularly if the targets of those attacks are groups or countries disfavored by the governments in power.

What's more, the apparent strength of U.S. law, and presumably that of other advanced industrialized countries, is somewhat beside the point in the absence of both the jurisdictional reach and investigative nimbleness needed to bring criminal cases against the most dangerous actors. Neither of these conditions exists today, nor are they likely to exist in the foreseeable future. Rather, the near impossibility of the real-time attribution of many cyberattacks – combined with the fact that many cyberattacks come from places where American authorities cannot count on official cooperation – makes criminal laws the crudest of instruments for preventing attacks.

More fundamentally, it can often be difficult to know in real time whether the criminal laws even offer the right legal framework in which to consider a given cyberattack. At the outset of a cyberattack, it may be unclear whether the attacker is a state, an organized criminal group, a terrorist group or a lone individual. It may also be unclear from where the attack is emanating. And it may even be unclear how severe the attack is – or even whether it is occurring at all. Consequently, authorities may not know whether they are dealing with a crime, an act of espionage or an act of war. Indeed, cyberattacks are also complicated because the United States – and most other countries – have not forsworn their own use of them either as covert actions or in the context of warfare. Indeed, the United States may well have played some role in the Stuxnet attack on Iran and unquestionably maintains a very potent offensive capability for purposes of both cyberwarfare and espionage.

As a result, a host of thorny legal questions attend a cyberattack that may (or may not) emanate from a state power or a non-state group large and coherent enough to wage war.

For example, when is a cyberattack damaging enough to constitute a "use of force" in the eyes of international law and thus constitute a legitimate basis for a military response? And when is it merely espionage and, therefore, not a basis under international law for a military response?[4]

In short, while there is an increasingly developed legal framework for prosecuting cyberattacks once they have been attributed and where jurisdiction permits, as is the case in the biological arena, the law is falling farther behind rather than catching up with the problem.

6 Interactions with Other Megatrends

In thinking about the interaction between this set of problems and the other major trends under discussion in this study, it is useful to begin with the observation that all things interact at some ultimate tectonic level. The butterfly that flaps its wings and causes a breeze may ultimately somehow start a war. However, these interactions are often too diffuse to describe prospectively, and we cannot reasonably anticipate these higher-order effects. Just as it is a fool's errand to try to imagine global security a century out, it is also a mug's game to try to describe in detail, for example, the relationship over time between cybersecurity, climate change and biodiversity. There will, no doubt, be *some* relationship – just as species diversity led to the existence of that butterfly that once fanned Napoleon's neck. And the relationship may even prove important. But to think that one can anticipate it is sheer hubris.

Accordingly, we should begin considering megatrend interactions by dividing the trends into three categories: those whose interactions with the matters at issue in this paper one might reasonably anticipate; those one might describe in vague terms but about which any detail is implausible; and those about which one really cannot say anything useful at all.

This latter category has, as I have indicated, one obvious member with which we can dispense up front: I can envision only the most diffuse connections between the security problems I have described and the problems of biodiversity taken up in the contribution by Wolfgang Cramer and Katrin Vohland in this volume. One can, to be sure, hypothesize potential interactions; for example, it might be that the therapy for some engineered pathogen will be found in a species whose existence is threatened by climate change. And perhaps the governance changes necessary to protect society against individual bad actors wielding powerful new technologies will somehow facilitate the governance changes needed to bring carbon emissions under control. After all, both issues involve enormous problems demanding international collective action and, specifically, the question of how the United States and China will engage with each other over time. One can point out that both are likely to be significant features of a vastly complicated U.S.-China relationship

4 For an excellent discussion of these and other related questions, see Chapter 7 of Owens, Dam and Lin 2009.

and that, therefore, they might well both follow the larger trajectory of that relationship. A closer, more cooperative U.S.-China relationship over time will likely produce, at once, fewer cyberattacks, greater cooperation in cyber- and bio-security, and greater progress in reducing carbon emissions. Conversely, a world in which these two giants attack one another's computer infrastructure – or allow their citizens do so – on a daily basis is probably also a world less conducive to progress on global environmental issues.

More broadly, I suppose, we can also hypothesize certain causal chains between developments in one area and in the other. For example, we can imagine that losses in biodiversity will produce huge economic and financial losses, as the Cramer-Vohland contribution envisions, and that these will increase human misery and thereby create more of precisely the sort of disaffected people most inclined to causing mayhem on wealthier parts of the world. The trouble is, however, that we can just as easily describe interactions producing precisely the opposite effect – that is, that losses in biodiversity would lead to economic damage that would, in turn, lead to a lessened pace of technological progress. This slackening of technological development could, in turn, reduce the degree to which governments lag behind the technological curve.

The point is that any effort to imagine these interactions in any detail involves rather rank and unuseful speculation. Beyond the blandest observation that the two trends will interact, we can confidently say almost nothing about how they will do so over time.

We can, perhaps, be somewhat more specific with respect to energy and natural resources – though not all that much more specific. On the assumption that Brown and Darmstadter are correct in their contribution to this volume that "(the) ability to generate an inclusive economic well-being will be governed to a great extent by our ability to overcome resource scarcity while reducing pollution and greenhouse gas emissions," this point obviously has significant implications for the security concerns I have outlined here. An "inclusive economic well-being," after all, is certainly key in general terms to reducing security threats. The more people the world has who are profoundly dissatisfied and for whom the global economy does not provide, the more people there will be with an incentive to attack the world. Generally speaking, while wealth-generation and increased economic opportunity will promote security, poverty and hopelessness – by creating more disaffected people with a sense of gross injury – will tend to push in the other direction. It follows that a world with broad energy scarcity and persistent conflicts over natural resources will be a less secure world than one in which energy's abundance makes fighting over resources unnecessary. And it also follows that a world with more conflict will have more individuals inclined to take those conflicts into their own hands than will a world with less conflict.

To be sure, a world of resource and energy abundance will by no means eliminate the security problems I have described here. Crazy individuals and small groups of technologically capable malcontents will exist no matter what our energy future looks like. Some of them will succeed at doing terrible things. But the question of how many there are is important. Isolated, occasional events – no matter how horrible – are almost by definition manageable. They cause death and chaos, and then we adjust. But having lots of people wanting to cause mayhem, and capable of doing so, makes society ungovernable. Thus,

the number of major friction points alienating individuals matters a great deal. The general subject of energy and natural resources could clearly be one of these major friction points.

The trouble is that, while it is relatively easy to imagine the connection between these two trends at the most abstract level, envisioning the connection at that level of abstraction does not give rise to many – or any – useful analytical or policy approaches. Instead, it simply suggests that it would be a whole lot better to solve our resource and energy problems than to not solve them, which is obvious in any event for a great many other reasons.

The demographic trends discussed in Jack Goldstone's contribution to this volume offer a similarly obvious set of interactions – with similarly few action items. Anyone worried about the issues I have discussed here will read with a gnawing feeling in his or her stomach a projection of "a concentration of large, youthful populations on the move in an 'arc of instability' reaching from southern Africa through the Middle East as well as South and Southeast Asia." Hardly less worrisome is the dramatic drop Goldstone projects in the demographic weight of advanced countries – presumably the places in the world with the least disaffected populations and the greatest governance capacity – and the "concentration of near-term population growth in regions with relatively poor populations, fragile or ineffective governments, and especially high vulnerability to climate change."

When considering the implications of the proliferation of dramatically empowering technologies to individuals all over the world, a huge demographic bulge in precisely those parts of the world that are the most disaffected and worst-governed has to magnify one's fears of the problem – and probably by a lot. Other trends Goldstone points to push in similar directions, such as a decline in the relative military capacity of the West. More generally, we should take no comfort from his warning that "[i]f the economies of fast-growing developing countries do not start to close the gap with those of the richer countries, the standard of life enjoyed in the West will seem more elite and unfair than ever, thereby fueling resentment among developing-country populations against the more developed world." In the security environment I have described, broad resentment among developing-world populations has got to be among the scariest trends we can envision.

Here again, however, translating this interaction into anything more concrete than a generalized fear-magnifier is difficult. There are so many reasons to want to improve the standard of living for those in the developing world (not to mention for those in the not-yet developing world) that it seems quite superfluous to add to the list that there might be fewer people as a result of such economic development who are eager to trigger major bio- and cybersecurity events. As Goldstone makes clear, the demographic trends he describes are not negotiable at this stage; they will happen. So it's not like we can, with quick and decisive policy action, make growth continue in advanced democracies and prevent it in the "arc of instability" until that arc becomes a bit less unstable. Goldstone's analysis should, in my view, be taken as a warning that my earlier suggestion about plenty of people wanting to use technology to cause mayhem will likely grow more rather than less true as the century goes on. But I'm not sure we can say more about the interaction than that.

We come, then, to the two megatrends whose interactions with the security matters at issue here are most concrete. The first of these is economic globalization; the second is global governance. I treat these two megatrends together because, for present purposes, they really aren't severable. The security issues I have identified are centrally problems of globalization. If they have resolutions, those resolutions lie in governance. And since those problems are inherently international, effective governance will not plausibly emanate from a single state but, rather, will necessarily involve a significant measure of global cooperation.

Greater global economic integration is inevitable. This means that the greater, faster and wider international proliferation of technologies developed in the civilian sector is also inevitable. Once technologies demonstrate their value, dependence on them will spread like wildfire and exploitation of them – for good and ill – will spread quickly, as well. The Internet will guarantee an essentially unimpeded flow of knowledge concerning both the positive and negative uses of those technologies. There is no real doubt that this will happen. The only real question, in my view, is the pace at which it will happen. Does the knowledge curve keep rising exponentially, or does it begin leveling off? Does the trade in radically empowering technologies globalize in a largely uninhibited fashion – as it has to date with computers, encryption and biotech – or do regulatory regimes emerge that impede it to some degree?

To be sure, the entirety of the security problem I have described does not emanate from globalization. After all, the wide dissemination of radically empowering technologies even *domestically* would alone pose serious challenges. But the pace and scope of globalization is key to the degree to which the problem magnifies. Globalization has already translated it in both the biotech and cyber-security arenas from a set of challenging domestic-security issues into issues of international governance and security. The greater the international flow of this category of technologies – that is, the less borders come to matter in our economic lives over time – the more we can expect to see this pattern replicated across other platforms.

Likewise, the more this comes to pass, the more obvious it will also be that any plausible governance of these platforms must cross borders as well. The degree to which this problem proves manageable ultimately hinges to some extent on whether the world can find effective governance systems to manage these platforms. Unfortunately, there is little reason to believe that the world will develop the kind of strong governance structures that would offer grounds for particular optimism.

Among the range of possibilities presented by Bruce Jones, for example, in his contribution to this volume, one can envision the global governance challenge as anything from extraordinarily difficult to utterly hopeless – which isn't very promising. The most hopeful scenario he outlines is the re-establishment of U.S. hegemony in the coming years. In that scenario, the problem of international governance of this space becomes a complex matter of American leadership – with the United States pushing other countries to develop investigative capacity, to adopt serious legal regimes and to cooperate in the attribution of attacks and potential responses. This is an enormously challenging project, particularly since many countries will actively resist U.S. leadership in these arenas, as they

do in others. I can imagine easily enough broad international cooperation on responses to disease outbreaks. However, it is far harder to imagine that even U.S. hegemony at its most hegemonic could induce routine collaboration on cybersecurity from countries that use cyberattacks as a matter of statecraft – particularly since the U.S. itself doesn't disclaim the use of such attacks. In other words, even in this most optimistic scenario, the prospects for international governance are poor.

The problem grows immeasurably harder in either of the other two scenarios Jones describes. A world of U.S.-China bipolarity would likely not lend itself to collaborative international governance in these areas. Rather, the competitive jockeying between the two powers in many areas will likely inhibit governance. The cyber arena already illustrates this point clearly: Neither side is likely to reveal either its offensive or defensive capabilities to the other, and both want deniability for the attacks they do undertake. These facts will limit any serious efforts at international governance. And such problems will compound many times in Jones's third scenario: a world of true multipolarity. It is hard to imagine any significant international governance of this type of problem under those conditions.

To be candid, however, it jumps the gun a bit to discuss the *international* governance dimensions of the problem of radically empowering technologies, for we first need to consider an important antecedent question: Are these problems governable even in the sovereign territory of a strong state? To put it bluntly, as the earlier survey of governance in the U.S. to date shows, there just aren't that many promising options for managing these issues. And this fact gives rise to what I suspect will be the most important interaction between this class of technologies and governance – both transnationally and nationally. Specifically, it stands to bring about a substantial erosion of a government's monopoly on security policy, putting in diffuse and private hands for the first time responsibility for protecting nations from one another and from their own citizens.

There are people who would write that sentence with joy in their hearts. I am not one of them. If one takes the function of the democratic state as securing for citizens terms of ordered liberty, the capacity to defend a nation against attack is a core function with which we interfere at our peril. "Power to the people!" is a slogan that has always rung to me of gridlock, at best, and of mob rule, at worst.

That said, I'm not sure how the basic presumption about security remaining a governmental function holds up in the face of the rapid development of this class of technologies. This point is perhaps most vivid in the cyber arena, where, as I noted above, a huge amount of traffic into and out of the United States – including government traffic – now takes place over privately owned lines, and the government quite literally does not control the channels through which attacks can occur. But this is also true in the biotechnology sphere. Since the revolution has taken place largely in private rather than the government's hands, the government employs only a fraction of the capable individuals. Thus, the capacity to respond to or prevent an attack is as diffuse as the capacity to launch one. We have already seen this effect with the 2010 oil spill in the Gulf of Mexico resulting from the explosion of the "Deepwater Horizon" drilling rig. If a spill of this magnitude were launched intentionally, rather than by accident, nobody would doubt that its magni-

tude rose to the level of an act of war. Yet, in this case, the U.S. Navy had no capacity to respond to it and deferred to British Petroleum to stop the "attack." In other words, the development of non-classified, civilian technologies by private-sector outlets caused the United States to subcontract the defense of its shores and territorial waters to a multinational corporation.

There is a ray of hope in this otherwise bleak picture – though how significant a ray it is remains to be seen. The technological revolutions at issue here have given enormous numbers of people the capacity to do great harm, but they have also given enormous numbers of people the capacity to work to prevent that same harm. The proliferation of defensive capabilities has been every bit as rapid as the proliferation of offensive capabilities – indeed, exponentially more so since the good guys so vastly outnumber the bad guys. The individual scientist had no ability to prevent the Soviet Union from launching a nuclear attack against the United States or from invading Western Europe. But the individual scientist, and groupings of individual scientists, have an enormous role in biosecurity – from driving the further innovations that can wipe out infectious diseases, to spotting the security implications of new research, to reporting on colleagues engaged in suspicious activities out of sight of the authorities. The same is true of cyberspace. The number of actors capable of playing a significant role in the solution grows far more quickly than the number of people capable of creating the problem.

This fact will, I suspect, tend to force changes in the governance structures of security – both domestically and globally. Here, I don't mean that any kind of formal doctrinal shift will take place and that notional power will migrate to private actors. The change will be far subtler than that. As the powers we have traditionally granted to government actors grow less plausible as tools for the problems they confront, aspects of our security policies will tend to decentralize to those actors better-positioned to have real impact. Nobody's going to rewrite American or European constitutions to vest security responsibilities in nongovernmental actors. It will just happen. As governments find themselves relatively feckless in the face of the problem and other actors find themselves capable of responding, we will start thinking about those other actors as bearing important security functions for which we once looked to government. And, I suspect, governments themselves will end up playing more of a coordinating role with respect to these other actors than has been the case with the classic "defend-the-borders" model of security. Just as we found ourselves waiting for BP to solve the problem it created in 2010 – though that problem was clearly a national-security matter – we will someday find ourselves asking telecommunications giants, such as Verizon or AT&T, to address a foreign attack on American infrastructure.

This fact pulls the mind back toward themes and ideas developed in the context of the debate over intellectual property. A major current of this body of thought involves the protection of legal space for communities of various sorts to use and borrow one another's ideas and work in collaborative efforts to build things. Boyle's recent book, for example, contains a spirited defense of distributed applications, such as file sharing, of the open-source software movement and of Creative Commons licenses (Boyle 2008: 179–204). Indeed, the world has seen amazing demonstrations of what large groups of people can

do when they pool expertise – even with very limited coordination. The most famous example is Wikipedia, but this is far from the only one. Anyone who has used Open Office – an open-source alternative to the Windows Office application suite – knows that it doesn't take a major software company to produce a major piece of software. Indeed, it is an interesting fact – and highly salient for our purposes here – that open-source software is often more stable and secure than proprietary code (Schneier 2000: 343–345). While this point has its dissenters, the famous line in the open-source software movement that "given enough eyeballs, all bugs are shallow" may have real application not just to computer bugs, but to viral ones, as well (Raymond 1999).

Given that security will be – to borrow a term from this lexicon – a more distributed application than it has been in the past, we ought to start thinking about it as such. And, here, the landscape actually seems somewhat promising. As I have noted, there are many more good guys than bad guys both on the Internet and in the biotech world. They are enormously innovative, and they are much closer to the ground than any government is. They offer a great deal of capacity to identify the bad guys and to develop countermeasures to their actions, and they make up a huge reservoir of thought and expertise in the development of strategies for both responses and prevention. Governments' role in protecting us from attacks may be more the coordination of large numbers of people than the direct security function we are used to seeing them play. This evolution toward distributed security, I suspect, is our future over the coming century – or, at least, one unnerving component of it.

References

AEDPA (Anti-Terrorism and Effective Death Penalty Act of 1996). April 24, 1996. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ132.104.pdf.

Antolin-Jenkins, Vida M. "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?" *Naval Law Review* (51) 10: 132–174, 2005.

Applebaum, Anne. "For Estonia and NATO, a New Kind of War." *The Washington Post* May 22, 2007. www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html.

Baker, Stewart. *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism*. Stanford, Calif.: Hoover Institution Press, 2010.

Boyle, James. *The Public Domain: Enclosing the Commons of the Mind*. New Haven, Conn.: Yale University Press, 2008.

Bridis, Ted. "CIA: Hackers Demanding Cash Disrupted Power." *The Associated Press* January 28, 2008. www.msnbc.msn.com/id/22734229/.

Brown, DeNeen L. "Teen Admits Attacking Web Sites." *The Washington Post* Jan. 19, 2001. E1.

Bügl, Hans, John P. Danner, Robert J. Molinari, John T. Mulligan, Han-Oh Park, Bas Reichert, David A. Roth, Ralf Wagner, Bruce Budowle, Robert M. Scripp, Jenifer A.L.

Smith, Scott J. Steele, George Church and Drew Endy. "DNA Synthesis and Biological Security." *Nature Biotechnology* 25: 627–629, 2007.

BWATA (Biological Weapons Anti-Terrorism Act of 1989). Public Law 101–298. May 22, 1990. http://thomas.loc.gov/cgi-bin/query/z?c101:S.993.ENR:.

BWC (Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction). April 10, 1972. www.opbw.org/convention/conv.html.

CDC (Centers for Disease Control and Prevention). Notice for Proposed Rulemaking to amend CFR Parts 70 and 71. 70 Federal Regulation 71892–71948. November 30, 2005.

Cello, Jeronimo, Aniko V. Paul and Eckard Wimmer. "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template." *Science* (297) 5583: 1016–1018, 2002.

Chyba, Christopher F. "Biological Terrorism and Public Health." *Survival* (43) 1: 96–97, 2001.

Chyba, Christopher F. "Toward Biosecurity." *Foreign Affairs* (81) 3: 122–136, 2002.

Chyba, Christopher F. "Biotechnology and the Challenge to Arms Control." *Arms Control Today* (30): 11–17, 2006.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, N.Y.: HarperCollins, 2010.

Council of Europe. Convention on Cybercrime Ratification and Signature List. n.d. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Council of Europe. Convention on Cybercrime. November 23, 2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

van Creveld, Martin. *Nuclear Proliferation and the Future of Conflict*. New York, N.Y.: Free Press, 1993.

Cunliffe-Owen, F. "Death of Francis Ferdinand Makes for Peace of Europe." *The Sun* (New York) June 29, 1914.

FBI (Federal Bureau of Investigation). Bioterrorism Security Risk Assessment Form. n.d. www.fbi.gov/about-us/cjis/bioterrorism-security-risk-assessment-form/bioterrorfd961.

Fearon, James. "Catastrophic Terrorism and Civil Liberties in the Short and Long Run." Paper presented at a symposium on "Constitutions, Democracy, and the Rule of Law" held during Columbia University's 250th anniversary celebrations. October 17, 2003. www.stanford.edu/~jfearon/papers/civlibs.doc.

Gerstein, Josh. "Obama Team Mulls New Quarantine Regulations." *Politico* August 5, 2009. www.politico.com/news/stories/0809/25814.html.

Goodman, Seymour E., and Herbert S. Lin (eds.). *Toward a Safer and More Secure Cyberspace*. Washington, D.C.: National Academies Press, 2007. http://books.nap.edu/catalog.php?record_id=11925.

Gostin, Lawrence O., Jason W. Sapsin, Stephen P. Teret, Scott Burris, Julie Samia Mair, James G. Hodge Jr. and Jon S. Vernick. "The Model State Emergency Health Powers Act: Planning for and Responding to Bioterrorism and Naturally Occurring Infectious Diseases." *The Journal of the American Medical Association* (288) 5: 622–628, 2002.

Graham, Bradley. "U.S. Studies a New Threat: Cyber Attack." *The Washington Post* May 24, 1998. A1. www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm.

Graham, Bradley. "Hackers Attack Via Chinese Websites." *The Washington Post* August 25, 2005. www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

Green, Leslie C. *The Contemporary Law of Armed Conflict*. 3rd ed. Manchester: Manchester University Press, 2008.

Gross, Leo. "The Peace of Westphalia, 1648–1948." *American Journal of International Law* (42) 2: 20–41, 1948.

Jackson, Ronald J., Alistair J. Ramsay, Carina D. Christensen, Sandra Beaton, Diana F. Hall and Ian A. Ramshaw. "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox." *Journal of Virology* (45) 3: 1205–1210, 2001.

Kellman, Barry. "Biological Terrorism: Legal Measures for Preventing Catastrophe." *Harvard Journal of Law and Public Policy* (24) 2: 417–461, 2001.

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton, N.J.: Princeton University Press, 1999.

Lewis, James A. "Computer Espionage, Titan Rain and China." Presentation for the Center for Strategic and International Studies, Technology and Public Policy Program. Dec. 14, 2005. http://csis.org/publication/computer-espionage-titan-rain-and-china.

Lewis, James A. "Cyberattacks Explained" Presentation for the Center for Strategic and International Studies. June 15, 2007. http://csis.org/files/media/csis/pubs/070615_cyber_attacks.pdf.

Meserve, Jeanne. "Staged Cyber Attack Reveals Vulnerability in Power Grid." *CNN.com* Sept. 26, 2007. www.cnn.com/2007/US/09/26/power.at.risk/index.html.

Minshull, Jeremy, and Ralf Wagner. "Preventing the Misuse of Gene Synthesis." *Nature Biotechnology* 27: 800–801, 2009.

National Research Council. *Biotechnology Research in an Age of Terrorism*. Washington, D.C.: National Academies Press, 2004.

Nouri, Ali, and Christopher F. Chyba. "Proliferation-Resistant Biotechnology: An Approach to Improve Biological Security." *Nature Biotechnology* (27) 3: 234–236, 2009.

Owens, William A., Kenneth W. Dam and Herbert S. Lin (eds.). *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: National Academies Press, 2009. www.nap.edu/openbook.php?record_id=12651&page=R1.

PHSBPRA (Public Health Security and Bioterrorism Preparedness Response Act). 7 U.S. Code Sec. 8401. June 12, 2002. http://uscode.house.gov.

Rabodzey, Aleksandr. "Biosecurity Implications of the Synthesis of Pathogenic Viruses." *Politics and the Life Sciences* (22) 2: 44–49, 2003.

Raymond, Eric S. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, Calif.: O'Reilly Media, 1999. www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04.html.

Robb, John. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken, N.J.: John Wiley & Sons, 2007.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York, N.Y.: John Wiley & Sons, 2000.

Shane, Scott. "Critics of Anthrax Inquiry Seek an Independent Review." *The New York Times* September 23, 2008. www.nytimes.com/2008/09/24/washington/24anthrax.html.

Starr Jordan, David. "The Impossible War." *The Independent* February 27, 1913.

Svitkin, Yuri V., and Nahum Sonenberg. "Cell-Free Synthesis of Encephalomyocarditis Virus." *Journal of Virology* (77) 11: 6551–6555, 2003.

Taubenberger, Jeffery K., and David M. Morens. "1918 Influenza: the Mother of All Pandemics." *Emerging Infectious Diseases* (12) 1: 15–22, 2006. www.cdc.gov/ncidod/eid/vol12no01/05-0979.htm.

Tieman, Claus-Peter. "German Teenager Admits Creating Sasser Computer Worm." *The Associated Press* May 8, 2004.

Tumpey, Terrence M., Christopher F. Basler, Patricia V. Aguilar, Hui Zeng, Alicia Solórzano, David E. Swayne, Nancy J. Cox, Jacqueline M. Katz, Jeffery K. Taubenberger, Peter Palese and Adolfo García-Sastre. "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus." *Science* (310) 5745: 77–80, 2005.

U.S.A. Patriot Act. Public Law 107–56. October 26, 2001. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.

U.S. Code. http://uscode.house.gov.

U.S. Office of Technology Assessment. *Proliferation of Weapons of Mass Destruction: Assessing the Risk, OTA-ISC-559*. Washington, D.C.: U.S. Government Printing Office, 1993. www.au.af.mil/au/awc/awcgate/ota/9341.pdf.

Volchkov, Viktor E., Valentina A. Volchkova, Elke Mühlberger, Larissa V. Kolesnikova, Michael Weik, Olga Dolnik and Hans-Dieter Klenk. "Recovery of Infectious Ebola Virus from Complementary DNA: RNA Editing of the GP Gene and Viral Cytotoxicity." *Science* (291) 5510: 1965–1969, 2001.

Warrick, Joby, Marilyn W. Thompson and Aaron C. Davis. "Scientists Question FBI Probe on Anthrax." *The Washington Post* August 3, 2008. www.washingtonpost.com/wp-dyn/content/article/2008/08/02/AR2008080201632.html.

Wilson, Clay. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. Report. Washington, D.C.: Congressional Research Service, October 17, 2003. http://fas.org/irp/crs/RL32114.pdf.