Global Technology Regulation and Potentially Apocalyptic Technological Threats

Published in
Nanoethics: The Ethical and Social Implications of Nanotechnology
eds. Fritz Allhoff, Patrick Lin, James Moor, John Weckert
ISBN: 978-0-470-08417-5
Paperback
416 pages
August 2007

J. Hughes Ph.D.
Public Policy Studies Program
Trinity College
Hartford, CT 06106
860-297-2376
james.hughes@trincoll.edu

Abstract

In 2000 Bill Joy proposed that the best way to prevent technological apocalypse was to "relinquish" emerging bio-, info- and nanotechnologies. His essay introduced many watchdog groups to the dangers that futurists had been warning of for decades. One such group, ETC, has called for a moratorium on all nanotechnological research until all safety issues can be investigated and social impacts ameliorated. In this essay I discuss the differences and similarities of regulating bio- and nanotechnological innovation to the efforts to regulate nuclear and biological weapons of mass destruction. I then suggest the creation of a global technology regulatory regime to ensure the safe and equitable diffusion of genetic, molecular and information technologies, and point out the principal political obstacles to implementing such a regime.

Global Technology Regulation and Potentially Apocalyptic Technological Threats

"Dad, what if there is no future?"
Tristan Bock-Hughes, age 6

The Threat of Self-Replicating Technologies

In April 2000, Bill Joy, the chief technologist and co-founder of Sun Microsystems and inventor of the computer language Java, published a Luddite jeremiad in the unlikeliest of places, the militantly pro-technology *Wired* magazine. Joy had developed a serious case of anticipatory doom as he contemplated the potentially apocalyptic consequences of three technologies, genetic engineering, nanotechnology, and robots imbued with artificial intelligence. The key and qualitatively different threat that Joy saw in these technologies was that they all can potentially self-replicate. While guns don't breed other guns and go on killing sprees, gene-tailored plagues, future robots and nanophages can theoretically do just that.

Joy concluded that we need to return to the peace movement's effort to have all nations renounce the development of weapons of mass destruction, and apply it now to genetic, molecular and AI research. "These technologies are too powerful to be shielded against in the time frame of interest... The only realistic alternative I see is relinquishment: to limit development of the technologies that are too dangerous, by limiting our pursuit of certain kinds of knowledge" (Joy, 2000). Joy's call for relinquishment has had little effect on policy deliberation, but has added weight to the growing neo-Luddite movement against nano- and biotechnology. In this essay I want to both endorse Joy's concern over the potentially apocalyptic consequences of these emerging technologies and explain why Joy's proposal for global relinquishment of these technologies is not a useful proposal, and suggest a global regulatory alternative.

The Threat is Real

First, however, it is important to acknowledge that these technologies do pose potentially apocalyptic threats.

Bioweapons The intentional design of bacterial and viral weapons began in a large way in the 1960s in the U.S. and the Soviet Union. In the 1980s the techniques for recombinant redesign of viruses and bacteria became available, and those techniques were applied to smallpox and other vectors before the collapse of the Soviet scientific infrastructure. Today, many nations and organizations have access to the technical knowledge and tools necessary to begin a program of bioweapons research, and in particular experiments with genetic manipulation of biological agents (Williams, 2006; Chyba, 2006).

The genomes of influenza, plague, anthrax, SARS, pneumonia and other pathogens have been sequenced and are in the public domain. Using this information novel organisms could be designed to combine the virulence, latency and lethality of previous pathogens, to only attack specific races or body parts, or to be resistant to antibiotics and antiseptic methods. The Soviet bioweapons program explored combinations of strains of anthrax, smallpox, plague and Ebola (Williams, 2006). Warnings about gene-tailored bioweapons generated a biodefense program under the Clinton administration, and the terrorist attacks of September 11, 2001 and the 2001 anthrax attacks the bioterrorism threat galvanized expanded biosurveillance and biodefense initiatives from the Bush administration.

However, Joy is not only concerned with the intentional release of gene-tailored infectious agents designed as tools of mass destruction, but also with the accidental release of genetically engineered micro-organisms designed for benign purposes that might have similar catastrophic effects in our bodies or ecosystems. The key to effective gene therapy has been to find viral vectors sufficiently virulent that they would spread beneficial genes throughout the patient. Researchers have explored everything from the common cold to HIV as vehicles of gene transfer. Therapeutic success carries the risk that a gene-vector could spread, mutate and have unintended consequences. For instance, Australian researchers discovered that they had created a mousepox virus with 100% lethality (for mice) while trying to create a viral contraceptive (Nowak, 2001). Bacteria engineered to clean up oil spills could mutate to eat plastic. Biotech crops could slip out of their farms and wreak havoc on local ecosystems.

Nano Goos While the threat of nanomaterial pollution has already inspired calls for a moratorium on nanotechnological innovation (ETC, 2005), threats from self-replicating nanorobots are more speculative and farther in the future. Although this holy grail of a programmable nano-replicator is estimated to be several decades away, their eventual likelihood has generated much discussion of the apocalyptic scenario of “gray goo,” in which a set of replicators escape their programmed constraints and begin eating everything, destroying all life on Earth. According to one estimate (Freitas, 2000) nanobots could eat the Earth's biomass in about one week.

However, nanotechnologists have also demonstrated that rogue "ecophagous" nanorobots would likely starve, burn themselves up, or grow slowly enough to permit counter-measures (Freitas, 2000). Nano-engineers have proposed industry standards for making nanomachines dependent on specific resources, or self-limiting in their replication, to prevent outbreaks of nanoplagues (Foresight, 2000). Blue goo, i.e. nano-immune systems, could be deployed to detect and destroy gray goo. Nonetheless, the threats of widespread destruction through the intentional or accidental release of destructive nanomachines will eventually be real.

Killer Robots Finally, and most speculatively, Joy waxes eloquent about one of the oldest tropes of science fiction, that machine minds or robots might take over the world and destroy humanity: “superior robots would surely affect humans as North American placentals affected South American marsupials (and as humans have affected countless species)… biological humans would be squeezed out of existence” (Joy 2000).

Joy’s concern about self-willed, self-replicating robots is tied up with the extrapolations of Hans Moravec, Ray Kurzweil and others about the eventual emergence of machine minds. Computing power has doubled every 18 months for the last century, an observation dubbed Moore’s law. Maintaining that exponential growth rate, personal desktop computers will match the neural complexity of the human brain in the next decade. If self-awareness and other features of living minds are emergent properties of complex information processing, then there is already today a possibility of the spontaneous emergence of self-willed intelligence in machines since the complexity of all the information technology connected through the Internet has already reached human brain levels. While some assume that this will herald a new Golden Age, Joy is certainly not alone is assuming that the consequences of such an event would range from severely disruptive to apocalyptic.

Many critics have dismissed Joy’s concerns as “science fiction,” meaning they do not believe in the possibility of super-plagues, nanorobots and self-willed AI. But even if these threats are low probability we have to take seriously even the slightest threat of so huge a catastrophic effect. I agree with Bill Joy, ETC and the other advocates of technology bans that the apocalyptic threats from these technologies are very real and warrant dramatic action. But I disagree that technology moratoria are a practical proposal to address the risks of emerging technologies, since they cannot and will not be implemented. Apocalyptic technological risks can only effectively be reduced and prepared through effective transnational regulation, regulation which the Luddite critics do not believe would be adequate, and which the industrial and military sponsors of emerging technologies see as threats to their corporate and national security interests. In fact, as Joy points out, this dilemma has been with us since the advent of nuclear weapons: can we build an effective global infrastructure to ensure that we can accrue the benefits of dual-use technologies, such as nuclear power, without seeing a proliferation of their risks, i.e. nuclear weapons?

Governing the Proliferation of Dual-Use Technologies

If we accept that the threats from emerging technologies are in fact potentially apocalyptic, and relinquishment a quixotic proposal, it should be clear that advocacy of either voluntary scientific and industry self-regulation, or self-regulation by nation-states, is also an inadequate response. In the absence of effective global regulation codes of ethics and professional self-regulation are welcome first steps, and can provide crucial time for the formulation of global regulatory responses before the technologies proliferate, especially when the nations in the technological lead establish strict limits on the export of technologies of potential military significance as the United States does. But in the end, as with the regulation of nuclear, chemical and biological weapons, these threats require the creation of transnational regulations and agencies empowered to verify and enforce those regulations. A brief examination of the history of arms control agreements and enforcement therefore is order to underline the difficulties that such transnational regulation faces when the technologies are “dual-use,” having both beneficial and destructive uses, and when corporations and nation-states are unwilling to compromise proprietary secrecy and national autonomy.

Lessons from Arms Control Regimes

Before the first atomic weapon was tested at the Trinity site in Nevada, Edward Teller announced calculations showing that the test could ignite Earth’s atmosphere in an uncontrolled chain reaction. Robert Oppenheimer was so troubled that he consulted his mentor, Arthur Compton, who suggested a risk/benefit calculation that losing the war to the Nazis would be the better bet if the risk of destroying the Earth’s atmosphere was 3 in a million or more. By the time of the test, the Trinity team had proven that igniting the atmosphere was a theoretical impossibility. But how much of an unlikely possibility is still too possible? How do we know when we have passed the three in a million chance, and is this even the appropriate level of risk to take with the future of life on the planet? How large must the potential rewards of some line of research be to gamble with human existence?

After World War Two many scientists and peace activists proposed a global renunciation of nuclear weapons. There was not then, nor has there been since, sufficient political support for disarmament to enforce such a ban given the perceived national security interests of the nuclear powers, and the lack of an effective global body for enforcing treaties. The growth of the nuclear power industry, which produces fissile materials which can be used in bombs by states or terrorists, also made clear that the regulation of nuclear proliferation would need to permit beneficial uses of the technology while discouraging nuclear weapons proliferation. In 1957, the United Nations responded to the dilemma by creating the International Atomic Energy Agency (IAEA).

The IAEA's principal charge has been to ensure the safety of nuclear power. Since the Nuclear Non-Proliferation Treaty (NPT) entered into force in 1970, however, the IAEA has increasingly been called on to investigate states which are using nuclear power generation as a cover for nuclear weapons programs. The IAEA investigated allegations of an Iraqi nuclear weapons program before and after the U.S. invasion in 2003, and is currently involved in investigating nuclear programs in Iran and North Korea. However, again, the weakness of transnational governance, in particular the inability of the UN to muster sufficient military and economic coercion to force Iraq, Iran or North Korea to cooperate with arms inspectors and obey international prohibitions on weapons-capable nuclear programs, contributed to the Bush administration multi-factored rationales for the disastrous invasion of Iraq, and the on-going brinksmanship with Iran and North Korea.

The difficulty of regulating weapons of mass destruction has by no means been limited to these "rogue states" however. Neither the United States nor Russia were ever willing to agree to "anytime, anywhere" inspections of nuclear facilities in the Strategic Arms Reduction Treaties of 1992 and 1993, and instead relied on other, far less certain forms of monitoring and verification. Similarly the U.S. and the Soviet Union refused to give international agencies a free hand to monitor and investigate labs with biodefense capabilities under the Biological Weapons Convention (BWC) which entered into force in 1975. Since the BWC had no investigatory or enforcement mechanisms discussions began in the 1990s to strengthen the treaty to allow spot inspections of biodefense facilities, among other measures. In 2001 the Bush administration, responding to concerns about the protection of proprietary biotech information and the secrecy of US biodefense research, withdrew the United States from the BWC. The BWC negotiations were also stymied by the insistence of developing countries that the regime facilitate their acquisition of biotechnology for peaceful purposes (Marchant and Sylvester, 2006).

These efforts to regulate nuclear, biological and chemical technologies to prevent their use as weapons of mass destruction show that complete prohibition of the technologies has never been politically feasible because of their dual, beneficial uses. The only progress, and that slight, has been with efforts to create agencies like the IAEA that monitor the safety of peaceful uses of the technologies while investigating and discouraging their weaponization. This is the same situation we face with the proliferation of nanotechnology, genetic engineering and artificial intelligence, which could cure diseases, provide new sources of energy, make cleaner and more efficient industrial processes, and generally provide a more prosperous future. Global bans on these technologies are as unlikely as they were with the nuclear and biological technologies.

Technology relinquishment is also impossible because of the need to pursue effective prophylactic and defensive measures to the use of emerging technologies by rogue states and terrorist groups. After the United States signed the Biological Weapons Convention in 1972, and Richard Nixon dismantled the U.S. chemical weapons program, the Soviet Union and a number of other signatories secretly expanded their bioweapon programs. Yet, with subsequent emergence of a robust biomedical infrastructure in the United States we have the capacity to respond to potential bioweapons through initiatives like the U.S. Bioshield initiative enacted in 2004. A complete ban on work with pathogens like smallpox, anthrax and Ebola would also inhibit research on development of effective bio-monitors, vaccines and antibiotics for those pathogens, as is being promoted through the Bioshield program. In fact, the need to conduct biodefense research was cited by the Bush administration in its withdrawal form the BWC in 2001. Similarly any comprehensive ban on nanotechnology or robotics would inhibit the ability of signatories to conduct defensive research on these technologies in anticipation of nano- and bioweapons deployed by non-signatory and non-compliant states, and non-state groups.

Relinquishment is also unattractive because the apocalyptic risks we face are not just from these technologies, but also from nature itself. In the calculation of the risks and benefits from emerging technologies there are apocalyptic risks on both sides.

Biodefense research has application not just to potential bioweapons but also to emerging infectious diseases such as SARS and avian flu. New bio- and nanotechnologies may reduce the human burden on the ecosystem by growing more food on less land with fewer resources, creating new and more efficient energy sources and industrial processes, as well as making human beings less vulnerable to the consequences of rapid climate change and natural catastrophes such as earthquakes, floods, hurricanes and asteroid impacts. Anti-aging research, based on the convergence of accelerating bio-, nano- and information technologies offers the promise of saving billions of lives that would be lost this century to aging-related diseases. At the margins of prediction, and over the course of decades, technological renunciation may be *more* existentially risky than technological progress. Nonetheless, with appropriate regulation we can reduce the risks and substantially improve the likelihood of the benefits.

Transnational and National Regulation

Emerging technologies must therefore be included in the existing regime of international arms control, and environmental and product regulation, and that regime must itself be strengthened. Trade in genetically modified plants and animals is subject to review by the Codex Alimentarius, a joint venture of the Food and Agriculture Organization of the United Nations and the World Health Organization, which establishes voluntary safety guidelines for trade in food and agricultural products. As potentially toxic substances, international trade in nanomaterials is subject to regulation under the World Trade Organization's Agreement on Sanitary and Phytosanitary Measures (Thayer, 2005). The Agreement *encourages* nations to base domestic regulation on the international standards developed by the Codex Alimentarius, but has no enforcement mechanism.

The sale of computing systems with the potential for self-willed intelligence are not currently subject to any international regulation other than intellectual property protection, although systems deemed to be of military significance, such as encryption algorithms, are barred for export by the U.S. Commerce Department. In so far as technologies can be used to produce weapons, UN Security Council Resolutions 1540 and 1673 requires all states to adopt measures to stop nonstate actors from gaining access to them, and to report on their steps to identify and prevent non-state actors' uses of these technologies.

Although some countries faithfully ensure that their domestic regulations are in compliance with these international agreements, most do not. Since the U.S. invasion of Iraq, which the Bush administration justified in part by Hussein regime's non-cooperation with arms control inspections, and the inability of the United Nations to compel Hussein's cooperation, this issue of strengthening the compliance mechanisms of international arms control agreements has become central in international diplomacy. In 2006 the issue is central to conflicts between Iran and North Korea, on the one hand, and the IAEA and world community on the other. The inability of the United Nations to mobilize force against Sudan permits Khartoum to obstruct international investigation of genocide in Darfur, and the insertion of peacekeeping troops to protect the Darfuri.

Despite the United Nations having more troops deployed under blue helmets then ever before, more than 100,00 personnel deployed in eighteen different areas, the UN peacekeepers remain ad hoc and underfunded. There has been little success in convincing the UN member states to permit the creation of a supranational force capable of enforcing world law.

Even though they are only sporadically complied with, international regulations themselves are also often weakened by the disproportionate influence of corporate and nation-state interests. The food safety regulations of the Codex Alimentarius are seen as inadequate by many NGOs, who point out that the body invites far more consultation from corporate spokesmen than from public health advocates and nongovernmental organizations. More charitably, negotiating international regulations is difficult, contentious and costly, and therefore often forced to a minimal level. Also the goal of protecting free trade from capricious and protectionist trade barriers is often in conflict with the "precautionary principle" demands of NGOs and some European nations. For instance, in 2006 the World Trade Organization is finalizing a ruling that the EU has no grounds to restrict import of genetically modified crops since they have no proof of their being unsafe. This sets a precedent for a similarly high bar for any national or regional efforts to restrict the proliferation of nanomaterials.

So the regime of technology regulation required for preventing the proliferation of technologies of mass destruction must go well beyond the existing, voluntary regulation of trade and arms control to create of international mechanisms to verify that nation-states implement international agreements, or else face compelling sanctions. An example of this level of world law and enforcement would be agreement under the Genocide Convention that countries permit international investigation of charges of genocide and that the United Nations Security Council will take action to prevent stop genocide. (Again, however, we have seen with the case of Darfur and the inability of the UN to go to war with Sudan how ineffective that agreement has been.) There are also the global intellectual protection agreements, monitored by the World Intellectual Property Organization and GATT, which oblige nation-states to investigate and stop domestic firms that violate global copyrights and patents, or else be subject to international sanctions.

The regulation of the threats of potentially apocalyptic technologies thus requires not only that the safety of emerging technologies be addressed by transnational agreements, but that these agreements create and support agencies capable of engaging in surveillance and verification at both the national and transnational level, with triggers for compelling enforcement mechanisms, from economic sanctions to military force.

Global Surveillance Mechanisms

The principal obstacle to the building of an infrastructure of global technology regulation, after unwillingness to forego the potential benefits of the technologies, has been, as noted above, the unwillingness of nation-states and firms to open their military and private labs to a robust regime of inspection and verification. With the even greater invasiveness required for effective monitoring of emerging technologies the threats to corporate and national sovereignty are compounded. Given the rapid escalation in the level of threat, however, transnational agreements to monitor and control dangerous technology will soon be on the international agenda again.

The level of monitoring for potential apocalyptic nanotechnology, biotechnology and AI will need to be even more invasive than the surveillance regime attempted for nuclear power under the IAEA. Amy Stimson of the Center for Strategic and International Studies has argued that it would be possible to build systems for monitoring biotech facilities that would permit verification of the Biological Weapons Convention without divulging proprietary or national security information (Stimson, 2004). Unfortunately such monitoring systems can inevitably be deceived, and even "anytime, anywhere" inspection has quickly become irrelevant as the size of the facilities necessary to conduct research and development has shrunk. Dangerous nanotechnology and biological research can be conducted in very small facilities, an order of magnitude less easily detected than the facilities necessary to build a nuclear weapon. The mobile, trailer-based Iraqi bioweapons labs turned out to have been a Bush administration fabrication, but they were nonetheless a possibility. In the case of artificial intelligence research the idea of a "facility" is completely irrelevant, and the surveillance of dangerous AI would need to be distributed throughout the global information infrastructure.

Global surveillance for the signs of dangerous and aberrant technology will thus require the creation of novel and highly automated systems with global reach. An example would be the system of satellite monitoring for the heat signatures of rogue nanotechnology in the wild proposed by Robert Freitas (Freitas, 2000). Another would be the World Health Organization's Global Outbreak Alert and Response Network which aims to rapidly identify new epidemic diseases, genetype the pathogens, and develop and deploy vaccines. The existing global network of public and private groups that monitor and fight computer viruses could similarly be coordinated with law enforcement and cyberwarfare agencies to monitor for the emergence of self-willed information architectures.

Another area for a global technology control regime would be the standardizing and monitoring of good laboratory practices and safety standards. Materials and specimens need to tracked and accounted for, laboratory records maintained, and laboratory workers properly trained and vetted. Harvard biologist George Church has proposed for instance that all DNA synthesizing devices, capable of rapidly "printing" novel DNA of novel microorganisms, be tagged with electronic locators, programmed to forbid the synthesis of dangerous pathogens, sold only to approved laboratories, and registered with an international authority (Church, 2005; Wade, 2005; Chyba, 2006). Global intelligence monitoring of scientific publications would permit the identification of researchers and lines of research that may yield potential threats.

In 2004, in response to a National Academy of Science report on the regulation of biotechnology to prevent bioterrorism, the Bush administration created the National Science Advisory Board for Biosecurity to advise federal departments and agencies that conduct or support research that could be used by terrorists on ways of reducing the risk of diffusion of dangerous materials and scientific knowledge. However these measures apply only to federally funded facilities in the United States. Transnational regulations that apply to private, academic and government researchers need to be devised to identify the specific kinds of scientific research which should be subject to pre-publication review and redaction by national and transnational authorities, and researchers and journals need to be educated about these guidelines (Purkitt and Wells, 2006).

It is interesting to note that the militant defender of emerging technologies, Ray Kurzweil, found a rare point of agreement with Bill Joy in 2005 when they published a joint statement in the New York Times condemning the publication online of the sequenced genome of the 1918 influenza virus, which they considered a recipe for bioterrorism. They wrote "We urgently need international agreements by scientific organizations to limit such publications and an international dialogue on the best approach to preventing recipes for weapons of mass destruction from falling into the wrong hands." (Kurzweil and Joy, 2005).

Open and Democratic Societies

All these surveillance activities, and especially any restrictions on scientific research and publication, raise grave questions about the balance of safety with freedom. However, although there will be trade-offs between safety and freedom, as there has always been, another way to frame the issue is to emphasize the importance of open and democratic societies as a precondition for effective transnational threat identification and control. The principal global threats are not from scientific activities that are public and known, but from secretive military research programs and non-state actors hidden in closed regimes. The freer and more transparent the society, the more likely that regulators will be able to identify emerging technological threats.

Trade unions and non-governmental organizations in liberal democratic societies complement and support the regulatory apparatus. Citizens of authoritarian regimes are unable to organize or express concerns about environmental toxins or suspicious patterns of disease. In open societies unions and civic organizations can assist in monitoring scientific research and raising the alarm when the public's interests are at risk. While citizen groups and diligent regulators in democratic societies are still often at a disadvantage in relation to the influence of corporate power and the military-industrial complex, they are at least still permitted to investigate, mobilize and publicize. Democratic societies also can create and tolerate relatively independent government technology advisory bodies, such as the former Office of Technology Assessment which advised the US Congress until dismantled in 1995.

More Science, Not Less

To many defenders of scientific progress a global technology regulatory regime like the one I have described will seem little better than a blanket ban on research. This “techno-libertarian” perspective sees an unfettered marketplace as the best, and safest guarantor of rapid scientific development. However the bulk of technological innovation in the 20th century has occurred in large academic, corporate and military laboratories, within the constraints of regulation, and not in unregulated entrepeneurs’ garages. By establishing national and international funds to develop safe, prophylactic and remediative technologies an effective regime of technology regulation can stimulate innovation more than it slows it.

More science will be needed to create the information technologies for the regime of surveillance of the computers, laboratories, industrial facilities, and the global ecosystem. Alongside our global immune system for computer viruses we need active immune system defenses, and rapidly deployable counter-measures for dangerous nanotechnology, robots and machine intelligence. The rapid convergence of the emerging technologies will bring with it novel solutions, such as the use of carbon nanotubes and sugar by a Clemson University team to coat and neutralize weaponized anthrax (Polowczuk, 2006).

Research should be devoted to engineering safety into the design of the technologies themselves. When Monsanto explored selling only sterile genetically engineered seed in order to protect its intellectual property rights it was condemned by environmentalists, even though these “Terminator” seed lines were precisely the best way to prevent genetic pollution. Self-replicating nanomachines can be designed to minimize the risk of mutation, and to require specific materials for reproduction (Foresight, 2000). Nanofactories can be built with encrypted black box software that forbids tampering, reverse engineering or the manufacture of dangerous substances and devices (Treder and Phoenix, 2003). Access to nanofactory source code would be restricted to engineers with proper vetting and oversight.

In the more difficult case of self-willed machine intelligence, fifty years ago Isaac Asimov proposed programming all artificial intelligence with an unalterable moral code, the “Three Laws of Robotics,” which required that a robot put the welfare of humans and obedience to humans above its own interests. But the messiness of self-reflexive minds capable of learning and changing, and the messiness of interpretability of specific moral dilemmas, means that efforts to encode these constraints into AI will probably only be as successful as moral education is for human beings. Noentheless information architectures with the capacity for self-awareness may be able to be designed with secure constraints and failsafes that can be used in the event of self-willed behavior.

Developing prophylactic and defensive technologies will, however, require a level of industrial policy and state subsidy that is currently out of favor in the United States, at least outside the military-industrial complex. Private industry cannot be relied on to participate in the necessary R&D without large public investments because the market for preventing a hypothetical apocalypse is not an attractive investment risk. With the exception of anti-virus software, which may offer private sector-based model for AI preparedness, there is no private market foreseeable for anti-nanotech measures or even pandemic vaccines and treatments. Indeed, two thirds of the deaths in the developing world are due to about a dozen infectious diseases – malaria, dengue, and so on - few of which receive research attention from the pharmaceutical industry since they would not be able to recover their investments by selling a vaccine or treatment in sub-Saharan Africa. It was the market failure in antiretroviral drugs, which were far too expensive for the majority of the world's poor with HIV, that led to the creation of the reasonably successful Global Fund for HIV, Malaria and Tuberculosis, to subsidize treatment in the developing world, and price reductions in the face of threatened abrogation of the intellectual property agreements.

Even the Bush administration's multibillion dollar Bioshield program, initiated in 2004 to entice pharmaceutical companies to develop vaccines and treatments for potential bioweapons, has been unable to attract pharmaceutical firms because they do not believe the products will be profitable enough since their principal market will be to governments for stockpiles. As a way around this dilemma Bioshield will be creating a Biodefense Advanced Research and Development Agency (BARDA) to institutionalize the relationship between biotech firms and the defense establishment in the way that the Defense Advanced Research and Development Agency (DARPA) does (Mackenzie, 2006), with incremental payments for reaching R&D goals.

In fact, private firms, which have both benefited from decades of public investment in basic science and which profit from these technologies with potentially catastrophic risks, should be asked to internalize the costs of new research into prophylactic measures through a targeted tax to support research into safe design and prohylaxis. We do not want to repeat the mistake of the 1980s Superfund, which used tax dollars to clean up closed factories' toxic sites, or the Price-Anderson Act, which gave a green light to nuclear power in the 1950s by providing a half billion dollars of public insurance for nuclear accidents without ensuring that the plants developed safe long-term nuclear waste management.

Conclusion

In 1947 Albert Einstein, sure that the advent of nuclear weapons had made the need for global governance inescapably obvious, addressed the new United Nations saying, "The final goal…is the establishment of a supranational authority vested with sufficient legislative and executive powers to keep the peace. The present impasse lies in the fact that there is no sufficient, reliable supra-national authority…There can never be complete agreement on international control and the administration of atomic energy or on general disarmament until there is a modification of the traditional concept of national sovereignty…"

In 2006 calls for the creation of powerful transnational agencies may sound as quixotic as calls for the complete abolition of emerging technologies through voluntary acts of conscience. However, the only way forward is the same way that we have addressed all previous technological threats, from toxic chemicals to dangerous cars: investigate, educate the public, create political pressure for new laws and regulatory agencies to enforce the laws, spend public dollars on research into safer technologies, and keep popular pressure on those agencies to prevent their weakening and cooptation. The qualitative difference with these emerging apocalyptic threats, as compared to unsafe drugs, cars and toasters, is that the regulation must be global and prophylactic. We cannot allow a potentially apocalyptic event to spur us into action. We must create this regime before the threats emerge.

Seventeen years ago the common wisdom was that we would have the Cold War well into the 21st century. Then the Soviet Union collapsed. Ten years ago the common wisdom was that capitalism would be unchallenged in the 21st century. Then a global anti-capitalist movement rose in city after city to protest the unaccountability of global financial institutions. Five years ago Islamic fundamentalism was thought by many pundits to be waning, and terrorist attacks their last protest against the end of ideology. Since 9/11 and the Iraq war there is no end in sight for Islamist insurgent violence and terrorism around the world.

So I do not think it utopian today to echo Einstein's calls for the creation of empowered supranational agencies capable of enforcing regulations on emerging super-technologies. Creating these institutions will require a global movement powerful enough to force reluctant corporations and nation-states to put global survival ahead of private and national interests. It will be as difficult as it has been since 1947. But we really have no other choice.

Bibliography

Associated Press. 2001. "Physicist Warns Humans About A.I.," *Seattle Times*, Sep 2. http://archives.seattletimes.nwsource.com/cgi-bin/texis/web/vortex/display?slug=hawking02&date=20010902

Bailey, Ron. 2001. "Rage Against the Machines: Witnessing the birth of the neo-Luddite movement," *Reason*, July. http://www.reason.com/0107/fe.rb.rage.html

Bostrom, Nick. 2001. Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards. Yale University Philosophy Department. http://www.nickbostrom.com/existential/risks.html

Church, George M. 2005. A Synthetic Biohazard Non-proliferation Proposal. May 21. http://arep.med.harvard.edu/SBP/Church_Biohazard04c.htm.

Chyba, Christopher. 2006. "Biotechnology and the Challenge to Arms Control," Arms Control Today. October.

Dann, Jack and Gardner Dozois, eds. 1988. *Nanotech*. New York: Ace Books.

Dertouzos, Michael. 2006. "Not by Reason Alone," Technology Review, Sept, (103)5: 26.

Drexler, K. Eric. 1986. *Engines of Creation: The Coming Era of Nanotechnology*. Anchor Press/Doubleday, New York. http://www.foresight.org/EOC/

Drexler, Madeline. 2001a. "Undermining International Bioweapons Controls," *The American Prospect*, 12(19): Oct 12.

_____. 2001b. "The Invisible Enemy," *The American Prospec*t, 12(19) Nov 5.

ETC. 2005. A Tiny Primer on Nano-scale Technologies ...and The Little BANG Theory. http://www.etcgroup.org/upload/publication/55/01/tinyprimer_english.pdf

Foresight Institute. 2000. "Foresight Guidelines on Molecular Nanotechnology, v3.7" http://www.foresight.org/guidelines/current.html

Forrest, David. 1989. Regulating Nanotechnology Development. Foresight Institute. 23 March. http://www.foresight.org/NanoRev/Forrest1989.html

Freitas, Robert A. 1999. *Nanomedicine, Volume I: Basic Capabilities*. Austin, Tex.: Landes Bioscience.

_____. 2000. "Some Limits to Global Ecophagy by Biovorous Nanoreplicators, with Public Policy Recommendations." Foresight Institute. April. http://www.foresight.org/NanoRev/Ecophagy.html

Garrett, Laurie. 1995. *The Coming Plague: Newly Emerging Diseases in a World out of Balance*. Penguin USA.

_____. 2001. *Betrayal of Trust: The Collapse of Global Public Health*. Hyperion.

Guillemin, Jeanne. 2001.*Anthrax: The Investigation of a Deadly Outbreak*. University of California Press.

Joy, Bill. 2000. "Why the future doesn't need us," *Wired*, April. http://www.wired.com/wired/archive/8.04/joy.html

Kurzweil, Ray and Bill Joy. 2005. “Recipe for Destruction,” New York Times, Oct. 17.

Kantrowitz, Arthur. 1992. "The Weapon of Openness," in *Nanotechnology Research and Perspectives*, ed. B.C. Crandall and James Lewis, MIT Press, Cambridge, Mass.:303-311.

Mackenzie, Debora. 2006. “Biodefence special: Fortress America?,” *New Scientist*, Oct 7: 18-21.

Marchant, Gary and Douglas Sylvester. 2006. “Transnational Models for Regulation of Nanotechnology,” Journal of Law, Medicine and Ethics. Fall. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=907161

McMahon, Scott. 1996. "Unconventional Nuclear, Biological and Chemical Weapons Delivery Methods: Wither the 'Smuggled Bomb,'" *Comparative Strategy* 15: 123-134.

Miller, Judith. 2001. “U.S. Seeks Changes in Germ War Pact,” *New York Times*, Nov 1.

Miller, Judith, Stephen Engelberg and William J. Broad. 2001. “U.S. Germ Warfare Research Pushes Treaty Limits,” *New York Times*, Sept 4. http://www.nytimes.com/2001/09/04/international/04GERM.html

Morris, Julian ed. 2000. *Rethinking Risk and the Precautionary Principle*. Butterworth-Heinemann.

National Science Foundation. 2001. *Societal Implications of Nanoscience and Nanotechnology*. March. http://itri.loyola.edu/nano/NSET.Societal.Implications/

National Institutes of Health. 2001. “NIH Guidelines for Research Involving Recombinant DNA Molecules.” http://grants.nih.gov/grants/policy/recombinentdnaguidelines.htm

Nowak, R. 2001. “Disaster in the making,” *New Scientist*, Jan 13.

Osterholm, Michael and John Schwartz. 2000. *Living Terrors: What America Needs to Know to Survive the Coming Bioterrorist Catastrophe.* Random House.

Polowczuk, Susan. 2006. Clemson researchers develop nanotechnology to stop weaponized anthrax in its tracks. Clemson News. October 2. http://clemsonews.clemson.edu/WWW_releases/2006/October/anthrax.html

Preston, Richard. 1998. “Statement for the Record by Richard Preston Before The Senate Judiciary Subcommittee on Technology, Terrorism & Government Information and the Senate Select Committee on Intelligence on ‘Chemical and Biological Weapons Threats to America: Are We Prepared?‘” April 22, 1998 http://www.senate.gov/~judiciary/preston.htm

_____. 1998. "The Bioweaponeers," *The New Yorker*, March 9:52-65. http://cryptome.org/bioweap.htm

Pueschel, Matt. 2001. "DARPA System Tracked Inauguration For Attack," U.S. Medicine. April. http://www.usmedicine.com/article.cfm?articleID=172&issueID=25

Purkitt, Helen and Virgen Wells. 2006. "Evolving Bioweapon Threats Require New Countermeasures," The Chronicle of Higher Education, Oct 6, 53(7): B18. http://chronicle.com/weekly/v53/i07/07b01801.htm

Reynolds, Glenn Harlan. 2002. Forward to the Future: Nanotechnology and Regulatory Policy. Pacific Research Institute. http://www.pacificresearch.org/pub/sab/techno/forward_to_nanotech.pdf

Rifkin, Jeremy. 1999. *The Biotech Century: Harnessing the Gene and Remaking the World*. Jeremy Tarcher.

Roco, Mihail C. 2006. Survey on Nanotechnology Governance. IRGC Working Group on Nanotechnology. Geneva.

Rosenberg, Barbara Hatch. 2001. "A way to prevent bioterrorism," *San Francisco Chronicle*, September 18, 2001.

Sale, Kirkpatrick. 1995. *Rebels Against the Future: The Luddites and Their War on the Industrial Revolution: Lessons for the Computer Age*. Reading, Massachusetts: Addison-Wesley Publishing Company.

Selden, Zachary. 1997. Assessing the Biological Weapons Threat. Business Executives for National Security. http://www.bens.org/pubs_0297.html

Stimson, Amy. 2004. "Resuscitating the Bioweapons Ban: U.S. Industry Experts' Plans for Treaty Monitoring," Center for Strategic and International Studies, November.

Sunshine Project, The. 2001. "The Biological Weapons Convention and the Negotiations for a Verification Protocol," April. http://www.sunshine-project.org/publications/bk2en.html

Thayer, James. 2005. "The SPS Agreement: Can It Regulate Trade in Nanotechnology?" Duke Law and Technology Review, 0015. http://www.law.duke.edu/journals/dltr/articles/2005dltr0015.html

Treder, Mike and Chris Phoenix. 2003. The Safe utilization of Nanotechnology. Center for Responsible Nanotechnology. http://www.crnano.org/safe.htm

Twibell, T.S. 2001. "Nano Law: The Legal Implications of Self-Replicating.Nanotechnology." http://www.nanozine.com/nanolaw.htm

Wade, Nicholas. 2005. "A DNA Success Raises Bioterror Concern," New York Times, Jan 12. http://www.nytimes.com/2005/01/12/national/nationalspecial3/12gene.html

Wejnert, Jason. 2004. Regulatory Mechanisms for Molecular Nanotechnology, Journal of Jurimetrics 44: 1-29.

Williams, Mark. 2006. "The Knowledge," Technology Review. March/April. http://www.technologyreview.com/printer_friendly_article.aspx?id=16485

Zelicoff, Alan P. 2001. "An Impractical Protocol," *Arms Control Today*, May 2001. http://www.armscontrol.org/act/2001_05/zelicoff.asp