



## Industry self-governance: A new way to manage dangerous technologies

**Stephen M. Maurer and  
Sebastian von Engelhardt**

### Abstract

Advanced technologies for making chemical, biological, and nuclear weapons can be purchased from hundreds of companies around the world. But negotiating treaties to regulate this trade would take years—and even then, many governments lack the will or resources to enforce them. Security experts often suggest that the United States could avoid these difficulties by encouraging industry to govern itself. Recent experience in the artificial DNA industry shows that this approach can yield large dividends. At the same time, officials need practical guidance about when private standards are possible and what government can do to promote them. The authors argue that private security standards work particularly well for industries in which manufacturers face massive fixed-cost investments, sell to large buyers, and face risk from intelligent adversaries. This profile fits most high-technology industries that security experts care about. The authors also discuss strategies that governments can use to promote, influence, and learn from private initiatives to regulate dangerous technologies.

### Keywords

artificial DNA, International Association Synthetic Biology, private security standards, synthetic biology

**F**ifty years ago, governments and defense contractors controlled most of the essential technologies for making weapons of mass destruction. The rise of civilian markets that specialize in selling advanced technologies for extracting nuclear fuels, synthesizing complex chemical compounds, and creating genetically engineered life forms has radically changed that situation. Take, for example, the new discipline of synthetic biology. Today, at least 60 companies worldwide can make artificial, gene-length DNA in whatever sequence their customers request. This is wonderful news for researchers, who have used the technology to create spectacular new organisms that secrete jet fuel or can be programmed to seek and destroy cancer cells. But what is to stop researchers from using the same technologies to make artificial smallpox? Given that university scientists have already used artificial DNA to resurrect

the polio and 1918 influenza viruses, governments are understandably worried that terrorists could soon replicate the most dangerous organisms known to humans.

The traditional Cold War solution to this kind of dual-use problem is government action—mainly formal regulations and treaties. But in truth, these methods have never been a complete solution. For one thing, negotiated treaties are always imperfect. More than 40 years ago, Western governments signed the Biological and Toxin Weapons Convention, knowing that its enforcement provisions were negligible. The result was massive cheating by the Soviet Union, South Africa, and Iraq—and a badly discredited treaty. Today, most scholars and diplomats argue that new confidence-building measures can repair the damage. But doing so will take years. Until then, industry self-governance may be the only game in town for controlling biotechnologies.

The world should be thankful that terrorists cannot make advanced biological or chemical weapons from scratch, as the Soviet Union once did. But the world is changing. Non-state actors can acquire sophisticated chemical and biological materials over the Internet. Moreover, the number of companies selling advanced biology and chemical technologies is exploding. Even in Western countries, no regulator can begin to keep track of, let alone control, the flood of transactions in dual-use materials and technologies. Worse still, the new technologies have migrated beyond the reach of US and European governments. For example, gene-length synthetic DNA is already manufactured in China, Taiwan, South Korea, and India.<sup>1</sup> Supposing that a multilateral

treaty controlling the sale of DNA is even possible, negotiating with that many countries would take years. And even then, many governments may not be willing or even able to regulate effectively.

The good news is that Washington understands that it needs new strategies to deal with the dual-use problem. But how, exactly, can it persuade industry to address security? When pressed, academics and policy makers often talk about organizing meetings to “engage” industry “stakeholders” in creating agreed security standards. But market standards don’t work that way. Bill Gates never asked whether Windows should be the world’s dominant software standard. The market decided—and those who disagreed with it got the short end of the economic stick.

Washington has always known that market incentives can undermine treaties and regulations. But over the past two decades, an opposing trend has also emerged: the creation of private standards that don’t fight the market, but enlist it. In this new world, businesses practice social responsibility not because they believe in it—although most executives do—but because opposing such measures puts their market share at risk. Private standards don’t have the power of government behind them—they can’t send offenders to prison—but they can threaten something that businesses fear almost as much: bankruptcy. And these new private standards can usually be implemented faster than government regulations. Better still, they ignore national borders. In a global market, it doesn’t really matter whether a company is based in Germany, the United States,

or China. The same bottom line exists everywhere.

### **The rise of industry standards**

Before the 1990s, industry self-governance was often a joke; companies promised standards and then promised to police themselves. In many cases, the ensuing “compliance” was little more than a publicity stunt. But modern standards are different. In the 1990s, large retailers like Nike and the Gap woke up to the fact that buying inventory from sweatshops and polluters would alienate the public—and, more important, put their market share at risk. The key to the new standards they developed in response was that retailers did not even pretend to police themselves; all they had to do was police others. One by one, the big retailers announced detailed social responsibility standards for their suppliers and cut off any company that defied them. Today, hundreds of such standards exist, and many retailers run massive enforcement programs that put government audits to shame.

At first, the new standards were limited to individual retailer supply chains. Soon, however, some companies began thinking about industry-wide solutions. This approach had obvious advantages in industries like deep-water drilling and genetically modified food, where a scandal involving one firm would likely harm the entire industry. Besides, maintaining multiple equivalent standards was costly. Probably the earliest example of a private, industry-wide standard came in 1990, when tuna canners StarKist, Chicken of the Sea, and Bumble Bee demanded that their suppliers adopt dolphin-safe technologies. Since then, worldwide dolphin mortality

has dropped 95 percent.<sup>2</sup> More recent successes include supermarkets’ industry-wide food standards. These include detailed requirements controlling how food is processed from the farm to supermarket. The requirements are backed by rigorous audits and surprise inspections.<sup>3</sup> Big coffee makers Kraft, Sara Lee, Tchibo, and Nestlé have likewise established an industry-wide collaboration that sets basic labor standards for growers. Particularly in Europe, governments have begun to take notice. German diplomats have been especially active in encouraging private standards for coffee and, more to the point for present purposes, artificial DNA.

### **Private biosecurity standards**

By the mid-2000s, large pharmaceutical firms were quietly asking what artificial DNA manufacturers had done to keep terrorists from placing orders. In April 2008, Germany’s leading artificial DNA trade group, International Association Synthetic Biology (IASB), convened a workshop to address the issue. The meeting ended with a public promise that members would, among other things, develop an industry-wide security standard. Within a few months, the association had prepared a draft code of conduct, which circulated widely among industry executives, government officials, and biological weapons diplomats. The document required human experts to compare incoming customer orders against known DNA sequences—a comparatively expensive procedure. In July 2009, IASB announced that it would finalize its code that November.<sup>4</sup> Two of the industry’s largest companies—DNA2.0 and

GeneArt—promptly announced what they called a fast and cheap alternative that replaced people with automation. The drawback, of course, was that computers must be told what to look for—and all existing threat lists are massively incomplete. That fact made the cheap solution far less capable of identifying DNA orders that could be used to make weapons. The argument became so heated that *Nature* magazine reported a “standards war” among DNA manufacturers (Hayden, 2009).

Like most Silicon Valley disputes, the biotech standards war ended quickly. By October 2009, the dissenters had quietly withdrawn their proposal and were negotiating a new consortium with three competitors. A month later, IASB finalized its code; shortly afterward, the consortium announced its own, comparably stringent “Harmonized Protocol.”<sup>5</sup> Since consortium members claim to possess more than 80 percent of the industry’s installed capacity for producing synthetic DNA, human screening had now been endorsed by essentially the entire industry.<sup>6</sup> The fact that two Shanghai firms signed the association’s code was particularly significant. Industry rumor had claimed for years that Chinese companies did little or nothing to screen orders. Endorsing the code helped put these stories to rest so Western customers could go on buying Chinese-made DNA with a clear conscience. Morality aside, the move was good for business.

There was, however, one last twist to the story: On November 27, the US Health and Human Services Department (2009) announced its own draft guidelines for regulating artificial DNA sales. Strangely, the new document—which asked DNA makers to compare

customer orders against a list of known, select-agent organisms—endorsed the same kind of fast and cheap methods that industry had just rejected as insufficient. While the document was later modified to make it clear that the government encouraged companies to adopt additional precautions against non-select agents (Health and Human Services Department, 2010), many industry executives seem to have taken the guidelines as a hint that private standards had lost their urgency. While both the consortium and IASB standards remain in place, there has been relatively little talk of new or extended self-regulation since.

### Building a theory

Synthetic DNA provides a particularly appealing case study of how private standards can protect the public while reducing industry’s own exposure to lawsuits and punitive regulation. That said, no single example can possibly tell government everything it needs to know. Among other things, officials need detailed guidance on when to promote new self-governance initiatives, how to engage existing ones, and how to coordinate private and public rule-making so that each reinforces the other. We, the authors, have attempted to fill these gaps by performing a detailed economic analysis that identifies the specific conditions under which private standards—a potentially powerful tool for regulating many WMD technologies—are likely to be effective (Engelhardt and Maurer, 2012).<sup>7</sup>

So why do companies want standards in the first place? Industry executives frequently point out that lawsuits could ruin them if, for instance, terrorists used

their products to kill civilians. This suggests that taking reasonable precautions makes good business sense. At the same time, many companies are small and can't pay large damage claims in any case. This suggests that owners may sometimes decide that it is cheaper to risk bankruptcy than adopt expensive precautions. Furthermore, many DNA manufacturers operate in places with weak legal regimes and may never be sued at all.

Fortunately, DNA manufacturers are not the only players interested in security. Customers also have a stake in preventing misuse. After all, big drug companies are counting on artificial DNA to help them discover new drugs that could earn (conservatively) \$1 billion each. That won't happen if a terrorist bio-attack—or even a near miss—frightens regulators into making artificial DNA illegal or prohibitively expensive. Paradoxically, many customers have a bigger stake in protecting artificial DNA than the makers themselves.

Better yet, these large corporate customers have power. This is because DNA makers face a dilemma. On the one hand, they face large fixed costs for research and development, equipment, and training. On the other, competition forces them to keep unit prices low. The bottom line is that DNA makers need high sales volumes to earn a profit. Inevitably, big customers know about this weakness and exploit it. This is typically done by naming “preferred suppliers” who promise to provide exceptional prices and service in exchange for a large book of business. Needless to say, this reward comes with an implied threat: The big customer can just as easily revoke the status if the preferred supplier fails to perform. For

the customer, shifting business to other vendors is a nuisance and may lead to slightly higher DNA prices. For the terminated supplier, however, the shift is a disaster. Lacking sales volume, the supplier's unit costs skyrocket. This cuts into profits and can force the company to raise prices so much that it loses still more sales. In some cases, the supplier can even become unprofitable and leave the industry entirely. In short, large synthetic-DNA customers possess enormous leverage for demanding price, quality, and any other terms they want. When they demand that suppliers practice self-governance, they are likely to get it.

There is also a corollary: Certain types of risk amplify customer leverage still further. Most people think of risk in terms of civilian industries, where the chance of accident increases with each additional unit produced. In economic terms, this kind of risk is a variable cost. National security risk, on the other hand, is different. Here, the number of sales to innocent buyers is completely irrelevant; the only thing that matters is how many terrorists are trying to turn DNA into weapons. More precisely, companies face the same terrorism risk no matter how many units they produce. Instead of being variable, terrorism risk adds to suppliers' fixed costs. Remarkably, then, self-governance turns out to be more stable for industries facing terrorism risk than, say, food safety or pollution issues.

The presence of dual-use risk also increases large customers' desire for self-regulation. Twenty years ago, companies like Nike usually focused on avoiding scandals in their own supply chain. What happened to other companies was secondary. By comparison, the

political and regulatory fallout from a terrorist scandal would cripple or eliminate artificial DNA technology across the economy. This means that it is no longer enough for large DNA purchasers to focus on their own supply chains; they also have to worry about every DNA manufacturer everywhere. Furthermore, large DNA purchasers almost always prefer more regulation than their smaller competitors.<sup>8</sup> Assuming that self-regulation is possible at all, we expect them to press hard for strong, industry-wide standards.

### **Practical advice**

It is not too soon to start thinking about how officials can put these economic insights to work. Our brief economic analysis offers important guidance: Private standards work best in industries that have high fixed costs, serve large customers, and face significant adversary risk. Industries in which customers already use preferred-supplier tactics to extract price and quality concessions are particularly good candidates for self-regulation. All of these factors were present in the synthetic DNA example above and are common in industries that produce high-tech products for the chemical and pharmaceutical industries.<sup>9</sup> This suggests that self-governance is a viable strategy for many WMD technologies.

Once policy makers decide that private standards are possible, they may have to encourage—or, in political parlance, jawbone—companies to act. These initial efforts should focus on the large downstream customers that possess leverage. Later, officials can turn their attention to the manufacturers themselves. Here, the goal should be less

to foster agreement, which the downstream buyers will demand in any case, than to encourage as many competing proposals as possible. The resulting “standards war” will almost always reveal important information. For example, some synthetic DNA companies warned the National Institutes of Health that stringent regulation would force them to shut down their US operations and send jobs overseas.<sup>10</sup> Conventional regulatory hearings could do little to disprove these assertions. By comparison, the fact that small, high-cost companies had already endorsed human screening immediately demonstrated that the big US firms could also afford it.

Policy makers may also want to influence the private standards debate. The most straightforward way to do this is by sharing data about known threats so industry can make intelligent cost-benefit judgments. Beyond this, officials may sometimes decide to steer industry standards in one direction or another. This can usually be done by endorsing particular proposals. Other, less honest methods (for example, deliberately withholding information) will deplete the government’s long-run credibility and should be avoided. The most difficult conflicts to resolve will usually come when private and public bodies develop standards in parallel. Such parallelism is desirable; it creates competition between standards and encourages information exchanges between the public and private sectors. Nevertheless, it also creates tension. On the one hand, strong private standards can reduce the political pressure for government regulation. On the other, public regulation can make private standards unnecessary. One partial solution to the problem



is for government regulations to trail private standards by six months or so. This practice allows officials to learn from, embrace, or overrule whatever private standards emerge.

Finally, officials should remember that private security standards can raise important antitrust issues. The reason is that strong industry-wide security standards almost always change an industry's risk and cost structure. Our analysis (Engelhardt and Maurer, 2012) shows that reducing industry-wide risk reduces fixed costs. This often helps weak firms to survive. Conversely, large and established firms could decide to oppose new standards because increased risk might injure new competitors. Security officials should work closely with antitrust advisers to prevent such tactics.

## **A promising tool**

At a minimum, diplomats should see private self-governance as a promising new strategy for achieving national goals. Although private standards are unlikely to replace traditional regulations and treaties, they can often extend them and are almost always worth considering. The fact that many large companies are based in the United States and Europe provides an added advantage.

But industry self-governance is more than a tactic. It can also make regulation more cost-effective. Governments seeking to regulate business activity often know very little about which standards are likely to be feasible or cost-effective. Customers in the private sector often overcome such problems by sharing and even delegating power to their more knowledgeable suppliers. This strategy is especially sensible for

complex technologies that no outsider can fully understand. For example, government officials often speculated that strong security standards for artificial DNA would be prohibitively costly. This may explain why their own draft guidelines were fairly lenient. While this thesis seemed reasonable at the time, officials should have realized their error as soon as industry voluntarily agreed to a higher standard. At that point, it would have been sensible for the government to lock in the industry result by revising its own draft guidelines upward.

Finally, US policy should promote industry self-governance for much the same reason that it encourages democracy in the developing world. Self-governance displaces chaos and, one can hope, empowers reasonable people. Furthermore, policy makers' experience with synthetic DNA and other industry initiatives to date has mostly been positive. This should encourage us to try further experiments.

## **Moving forward**

European diplomats have compiled a strong track record of engaging private standards in forestry, coffee, and synthetic DNA. For whatever reason, the United States has been more tentative, staying neutral in the synthetic DNA case and seemingly missing an opportunity to reinforce stringent controls on a potentially dangerous technology. Here, the cure seems straightforward: Officials who ignore the potential benefits of industrial self-governance should feel pressure to explain themselves. One way to increase this pressure is to create a political culture that stresses the importance of engagement. Statements

by high-level diplomats and respected bodies like the National Academy of Sciences would go a long way toward making this point.

If the power of private standards is to be fully realized, government officials will also need to adopt new attitudes. First and most obviously, they will have to decide when private standards are worth pursuing, either alone or as adjuncts to regulations and treaties. And when they do decide to pursue standards, government officials will need to show patience: While government can influence, industry will almost always have the final word. Even so, regulators will be amply repaid if business leaders use their power to bring new and better ideas to the table.

Industry self-governance is a reality. The only question is when the United States will start developing it as a diplomatic lever. Success will require new and explicitly economic habits of thinking: Policy makers will have to model their strategies on Bill Gates at least as much as on Henry Kissinger. For a diplomatic community that regularly talks about exercising “smart power,” that hardly sounds like too much to ask.

## Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Stephen M. Maurer conducted the work described in this article as a visiting scholar at the Institute for Advanced Studies in Toulouse.

## Notes

1. Markus Fischer, an International Association Synthetic Biology official, described the geographic distribution of gene-length synthetic DNA manufacturers in a personal exchange with the authors (March 21, 2013).

2. See Conroy (2007: 46); the International Marine Mammal Project’s “International ‘dolphin safe’ standards for tuna,” available at: [www.earthisland.org/imm/Dol\\_Safe\\_Standard.html](http://www.earthisland.org/imm/Dol_Safe_Standard.html); and the European Cetacean Bycatch Campaign’s “Tuna boycott which led to the ‘dolphin safe’ tuna label,” available at: [www.eurocbc.org/page322.html](http://www.eurocbc.org/page322.html).
3. See, for example, Fuchs and Kalfagianni (2010: 9) (“Retail food corporations” have “the power to govern”) and Campbell and Le Heron (2007: 142) (Australian farmers see private European food standards as a “large hurdle” for exports).
4. For a detailed history of private gene standards, see Maurer (2012) and Maurer and Fischer (2010).
5. The International Association Synthetic Biology’s (IASB) Code of Conduct for Best Practices in Gene Synthesis is available at: [www.ia-sb.eu/go/synthetic-biology/activities/press-area/press-information/code-of-conduct-for-best-practices-in-gene-synthesis/?keywords=code%20of%20conduct&tag=&searchSectionID=](http://www.ia-sb.eu/go/synthetic-biology/activities/press-area/press-information/code-of-conduct-for-best-practices-in-gene-synthesis/?keywords=code%20of%20conduct&tag=&searchSectionID=). The current, revised version of the International Gene Synthesis Consortium’s Harmonized Screening Protocol is available at: [www.genesynthesisconsortium.org/wp-content/uploads/2012/02/IGSC-Harmonized-Screening-ProtocolI.pdf](http://www.genesynthesisconsortium.org/wp-content/uploads/2012/02/IGSC-Harmonized-Screening-ProtocolI.pdf). Copies of the original document are available from the authors.
6. Because many gene synthesis firms are privately held, relatively little market-share information has been made public. However, the International Gene Synthesis Consortium has repeatedly said that its members possess about 80 percent of the industry’s installed capacity. See, for example, “IDT presents at Presidential Commission for the Study of Bioethical Issues: Representing the International Gene Synthesis Consortium and its ongoing work to prevent the misuse of synthetic genes,” available at: [www.idtdna.com/pages/docs/press-releases/2010-igsc](http://www.idtdna.com/pages/docs/press-releases/2010-igsc). Significantly, this number does *not* include gene synthesis companies that endorsed the IASB code or practiced human screening under their own independent standards.



- For this reason, readers should think of 80 percent as a lower bound; the actual adoption rate as of 2009 was almost certainly much higher.
7. Theoretical microeconomists use mathematical models to identify and understand the mechanisms that drive markets. Their basic strategy is to construct and solve equations in which simple, realistic assumptions (e.g., profit-maximizing firms, high fixed costs) lead to outcomes that are generically found in real industries. Readers should not confuse this exercise with the semi-empirical computer simulations that are used to predict, say, quarter-to-quarter fluctuations for the US economy. Instead, the goal is to construct mathematically rigorous theories that can be used to (a) disprove plausible but wrong arguments about how markets behave, (b) confirm and clarify correct intuitions, and (c) discover possible outcomes that the authors would not otherwise have thought of. This last virtue is particularly valuable for policy makers trying to imagine novel, “outside-the-box” strategies that have never been tried before. Our model posits an upstream high-tech industry that makes research tools that downstream companies use to invent new products. We analyze the case in which some large customers demand that upstream firms adopt strong, industry-wide security standards as a two-stage “game.” We solve this game to find that strong standards are stable under various conditions, i.e., that any upstream firm that defects from the high standard and specializes in making sales to customers that accept the lower standard will earn less profit. Full mathematical details can be found in section three of our study, available at: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2189919](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2189919).
  8. Customers who buy large quantities of DNA almost always do so because they are working on unusually lucrative uses like pharmaceuticals. This implies that they also have the most to lose if the technology is compromised.
  9. For a fuller discussion of the economics of gene synthesis and screening, see Maurer et al. (2009).
  10. One of the authors attended several meetings between 2006 and 2010 at which gene-synthesis executives made this claim to NIH and other government officials.

## References

- Campbell H and Le Heron R (2007) Supermarkets, producers and audit technologies: The constitutive micro-politics of food, legitimacy, and governance. In: Burch D and Lawrence G (eds) *Supermarkets and Agri-Food Supply Chains: Transformations in the Production and Consumption Of Foods*. Cheltenham: Edward Elgar. Available at: [www.cabdirect.org/abstracts/20083019302.html?sessionid=EAD33Fo606010169CoFD46D3312C1C10?gitCommit=4.13.20-5-ga6ado1a](http://www.cabdirect.org/abstracts/20083019302.html?sessionid=EAD33Fo606010169CoFD46D3312C1C10?gitCommit=4.13.20-5-ga6ado1a).
- Conroy ME (2007) *Branded! How the ‘Certification Revolution’ Is Transforming Global Corporations*. Gabriola Island: New Society.
- Engelhardt S and Maurer SM (2012) Industry self-governance and national security: On the private control of dual use technologies. Public policy working paper GSPP12-005, UC Berkeley Goldman School, December. Available at: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2189919](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2189919).
- Fuchs D and Kalfagianni A (2010) The causes and consequences of private food governance. *Business and Politics* 12(3). Available at: [www.degruyter.com/view/j/bap.2010.12.3/bap.2010.12.3.1319/bap.2010.12.3.1319.xml](http://www.degruyter.com/view/j/bap.2010.12.3/bap.2010.12.3.1319/bap.2010.12.3.1319.xml).
- Hayden EC (2009) Keeping genes out of terrorists’ hands. *Nature* 461(22). Available at: [www.nature.com/news/2009/090831/full/461022a.html](http://www.nature.com/news/2009/090831/full/461022a.html).
- Health and Human Services Department (2009) Screening framework guidance for synthetic double-stranded DNA providers. *Federal Register* 74(227): 62–319.
- Health and Human Services Department (2010) Screening framework guidance for providers of synthetic double-stranded DNA. *Federal Register* 75(197): 62–820.
- Maurer S (2012) Regulation without government: European biotech, private anti-terrorism standards, and the idea of strong self-governance. *Schriften des Münchner Centrums für Governance-Forschung* (Munich Center for Governance Research Publications Series).
- Maurer SM and Fischer M (2010) Harmonizing biosecurity oversight for gene synthesis. *Nature Biotechnology* 28: 20–22.
- Maurer S, Fischer M, Schwer H et al. (2009) Making commercial biology safer: What

the gene synthesis industry has learned about screening customers and orders. Available at: [gspp.dreamhosters.com/iths/Maurer\\_IASB\\_Screening.pdf](http://gspp.dreamhosters.com/iths/Maurer_IASB_Screening.pdf).

### Author biographies

**Stephen M. Maurer** holds appointments at the University of California's Goldman School of Public Policy and Berkeley Law School. Trained as a lawyer, he helped to develop and

finalize the International Association Synthetic Biology's Code of Conduct. Maurer is the editor and lead author of *WMD Terrorism: Science and Policy Choices* (MIT Press, 2009).

**Sebastian von Engelhardt** is an economist at the Friedrich-Schiller-University in Jena, Germany. His research focus is on intellectual property, open-source software, regulation in Internet markets, and self-governance.