PUBLISHED JANUARY 2003

Safe Utilization of Advanced Nanotechnology

by Chris Phoenix and Mike Treder

Abstract

Many words have been written about the dangers of advanced nanotechnology. Most of the threatening scenarios involve tiny manufacturing systems that run amok, or are used to create destructive products. A manufacturing infrastructure built around a centrally controlled, relatively large, self-contained manufacturing system would avoid these problems. A controlled nanofactory would pose no inherent danger, and it could be deployed and used widely. Cheap, clean, convenient, on-site manufacturing would be possible without the risks associated with uncontrolled nanotech fabrication or excessive regulation. Control of the products could be administered by a central authority; intellectual property rights could be respected. In addition, restricted design software could allow unrestricted innovation while limiting the capabilities of the final products. The proposed solution appears to preserve the benefits of advanced nanotechnology while minimizing the most serious risks.

Advanced Nanotechnology And Its Risks

As early as 1959, Richard Feynman proposed building devices with each atom precisely placed[1]. In 1986, Eric Drexler published an influential book, *Engines of Creation*[2], in which he described some of the benefits and risks of such a capability. If molecules and devices can be manufactured by joining individual atoms under computer control, it will be possible to build structures out of diamond, 100 times as strong as steel; to build computers smaller than a bacterium; and to build assemblers and mini-factories of various sizes, capable of making complex products and even of duplicating themselves.

Drexler's subsequent book, *Nanosystems*[3], substantiated these remarkable claims, and added still more. A self-contained tabletop factory could produce its duplicate in one hour. Devices with moving parts could be incredibly efficient. Molecular manufacturing operations could be carried out with failure rates less than one in a quadrillion. A computer would require a miniscule fraction of a watt and one trillion of them could fit into a cubic centimeter. Nanotech-built fractal plumbing would be able to cool the

resulting 10,000 watts of waste heat. It seems clear that if advanced nanotechnology is ever developed, its products will be incredibly powerful.

As soon as molecular manufacturing was proposed, risks associated with it began to be identified. *Engines of Creation*[2] describes one of the most famous: gray goo. A small assembler capable of self-replication could in theory replicate itself too many times[4]. If it were capable of surviving outdoors, and of using biomass as raw material, it could eventually devour the biosphere[5]. Others have analyzed the likelihood of an unstable arms race[6], and many have suggested economic upheaval resulting from the widespread use of free manufacturing[7]. Some have even suggested that the entire basis of the economy would change, and money would become obsolete[8].

Sufficiently powerful products would allow malevolent people, either hostile governments or angry individuals, to wreak havoc. Destructive nanomachines could do immense damage to unprotected people and objects. If the wrong people gained the ability to manufacture any desired product, they could rule the world, or cause massive destruction in the attempt[9]. Certain products, such as vast surveillance networks, powerful aerospace weapons, and microscopic antipersonnel devices, provide special cause for concern. Gray goo is relevant here as well: an effective means of sabotage would be to release a hard-to-detect robot that continued to manufacture copies of itself by destroying its surroundings.

Clearly, the *unrestricted* availability of advanced nanotechnology poses grave risks, which may well outweigh the benefits of clean, cheap, convenient, self-contained manufacturing. As analyzed in *Forward to the Future: Nanotechnology and Regulatory Policy*[10]*,* some restriction is likely to be necessary. However, as was also pointed out in that study, an excess of restriction will enable the same problems by increasing the incentive for covert development of advanced nanotechnology. That paper considered regulation on a one-dimensional spectrum, from full relinquishment to complete lack of restriction. As will be shown below, a two-dimensional understanding of the problem—taking into account both control of nanotech manufacturing capability and control of its products—allows targeted restrictions to be applied, minimizing the most serious risks while preserving the potential benefits.

Nanotech Manufacturing and Its Products

The technology at the heart of this dilemma is molecular manufacturing. A machine capable of molecular manufacturing—whether nanoscale or macroscale—has two possible functions: to create more manufacturing capacity by replicating itself, and to manufacture products. Most products created by molecular manufacturing will not possess any capacity for self-replication, or indeed for manufacturing of any kind; as a

result, each product can be evaluated on its own merits, without worrying about special nanotech risks. A nanotech-based manufacturing system, on the other hand, could build weapons, gray goo, or anything else it was programmed to produce. The solution, then, is to regulate nanofactories; products are far less dangerous. A nanotech-built car could no more turn into gray goo than a steel-and-plastic car could.

Some products, however, will be powerful enough to require restriction. Nanotech weapons would be far more effective than today's versions. Very small products could get lost and cause nano-litter, or be used to spy undetectably on people. And a product that included a general molecular manufacturing capability would be, effectively, an unregulated nanofactory—horrifyingly dangerous in the wrong hands. Any widespread use of nanotech manufacturing must include the ability to restrict, somehow, the range of products that can be produced.

If it can be done safely, widespread use of nanotech manufacturing looks like a very good idea for the following reasons:

The ability to produce duplicate manufacturing systems means that manufacturing capacity could be doubled almost for free.

A single, self-contained, clean-running nanofactory could produce a vast range of strong, efficient, carbon-based products as they are needed.

Emergency and humanitarian aid could be supplied quickly and cheaply.

Many of the environmental pressures caused by our current technology base could be mitigated or removed entirely.

The rapid and flexible manufacturing cycle will allow many innovations to be developed rapidly.

Although a complete survey and explanation of the potential benefits of nanotechnology is beyond the scope of this paper, it seems clear that nanotech has a lot to offer.

All of these advantages should be delivered as far as is consistent with minimizing risks. Humanitarian imperatives and opportunities for profit both demand extensive use of nanotechnology. In addition, failure to use nanotechnology will create a pent-up demand for its advantages, which will virtually guarantee an uncontrollable black market. Once nanotech has been developed, a second, independent development project would be both far easier and far more dangerous than the original project. The first nanofactory must be made available for widespread use to reduce the impetus for independent development[11].

Development of nanotechnology must be undertaken with care to avoid accidents; once a nanotech-based manufacturing technology is created, it must be administered with even more care. Irresponsible use of nanotech could lead to black markets, unstable arms races ending in immense destruction, and possibly a release of gray goo. Misuse of the technology by inhumane governments, terrorists, criminals, and irresponsible users could produce even worse problems—gray goo is a feeble weapon compared to what could be designed. It seems likely that research leading to advanced nanotechnology will have to be carefully monitored and controlled.

However, the same *is not true of product research and development.* The developer of nanotech-built products does not need expertise in molecular nanotechnology. Once a manufacturing system is developed, product designers can use it to build anything from cars to computers, simply by reusing low-level nanotech designs that have previously been developed. A designer may safely be allowed to play with pieces 1,000 atoms on a side (one billion atoms in volume). This is several times smaller than a bacterium and 10,000,000 times smaller than a car.

Working with modular "building blocks" of this size would allow almost anything to be designed and built, but the blocks would be too big to do the kind of molecular manipulation that is necessary for nanotech manufacturing or to participate in biochemical reactions. A single block could contain a tiny motor or a computer, allowing products to be powered and responsive. As long as no block contained machinery to do mechanochemistry, the designer could not create a new kind of nanofactory.

Once designed and built, a nanotech product could be used by consumers just like a steel or plastic product. Of course, some products, such as cars, knives, and nail guns, are dangerous by design, but this kind of danger is one that we already know how to deal with. In the United States, Underwriter's Laboratories (UL), the Food and Drug Administration, and a host of industry and consumer organizations work to ensure that our products are as safe as we expect them to be. Nanotech products could be regulated in the same way. And if a nanofactory could only make approved products, it could be widely distributed, even for home use, without introducing any special nanotech risks.

Nanofactory Technology: Regulating Risk, Preserving Benefit

It is generally assumed, incorrectly, that devices built with nanotechnology must be quite small. This has led to fears that nanotech manufacturing systems will be hard to control and easy to steal. In fact, as analyzed by Drexler and others in the field, the products of nano-scale mechanochemical plants can be attached together within the enclosure of a single device. Small building blocks can be joined to make bigger blocks; these blocks can be joined with others, and so on to form a product. This process is called convergent

assembly, and it allows the creation of large products from nano-scale parts. In particular, convergent assembly will allow one nanofactory to build another nanofactory. There is no need to use trillions of free-floating assembler robots; instead, the assemblers are securely fastened inside the factory device, where they feed the smallest conveyor belts.

A typical nanofactory might be the size of a microwave oven. Since the assemblers are fastened into the factory and dependent on its power grid, they have no need to navigate around the product they are building—this improves efficiency—and they have no chance of functioning independently. In addition, the entire nanofactory can be controlled through a single interface, which allows restrictions to be built into the interface. It can simply refuse to produce any product that has not been approved. (The improved security of tethered nanotech factories has been a theme in at least one work of science fiction[12].)

If a nanofactory will only build safe products, and will refuse to build any product that has not been approved as safe, then the factory itself can be considered safe. It could even build a duplicate nanofactory on request. With the restrictions built in, the second one would be as safe as the first. As long as the restrictions work as planned, there is no risk of gray goo, no risk of undesirable weapons or unapproved products, and no risk of producing unrestricted nanofactories that could be used to make bad products.

At the same time, products that were approved could be produced in any quantity desired. The products could even be customized, within limits—and the limits could be quite broad, for some kinds of products. If desired, the nanofactories (and the products) could have tracking devices built in to further deter inappropriate use.

With nanofactories that can only produce approved designs, the safety of nanotech manufacturing does not depend on restricting the use of the factories. Instead, it depends on choosing correctly which products to approve. The nanofactory itself, as a product, can be approved for unlimited copying. This means that the abundant, cheap, and convenient production capability of advanced nanotechnology can be achieved without the risks associated with uncontrolled nanotech manufacturing. A two-dimensional view of the risks of nanotechnology, *which separates the means of production from the products,* allows the design and implementation of policy that is minimally restrictive, yet still safe.

Using Nanotechnology Safely

A safe nanofactory design must build approved products, while refusing to build unapproved products. It must also be extremely tamper-resistant; if anyone found a way to build unapproved products, they could make an unrestricted, unsafe nanofactory, and distribute copies of it. The product approval process must also be carefully designed, to maximize the benefits of the technology while minimizing the risk of misuse. Restricted

nanofactories avoid the extreme risk/benefit tradeoff of other nanotech administration plans, but they do require competent administration.

One way to secure a nanofactory is to build in only a limited number of safe designs. The user could ask it to produce any one of those designs, but with no way to feed in more blueprints, the factory could never build anything else. This simple scheme is fairly reliable, but not very useful. It also poses the risk that someone could take apart the factory and find a way to reprogram its design library.

A more useful and secure scheme would be to connect the nanofactory to a central controller, and require it to ask for permission each time it was asked to manufacture something. This would allow new designs to be added to the design library after the nanofactory was built. In addition, the nanofactory would have to report its status back to the central controller. The system could even be designed to require a continuous connection; a factory disconnected from the network would permanently disable itself.

This would greatly reduce the opportunity to take the factory apart, since it could report the attempt in real time, and failed attempts would result in immediate arrest of the perpetrator. This permanent connection would also allow the factory to be disabled remotely if a security flaw were ever discovered in that model. Finally, a physical connection would allow the location of the factory to be known, and jurisdictional limits to be imposed on its products.

Current cryptographic techniques permit verification and encryption of communication over an unsecured link. These are used in smart cards and digital cellular phones, and will soon be used in digital rights management[13]. Using such techniques, each nanofactory would be able to verify that it was in communication with the central library. Only designs from the library could be manufactured. In addition, each design could come with a set of restrictions. For example, medical tools might only be manufactured at the request of a doctor. Commercial designs could require payment from a user. Designs under development could be manufactured only by the inventor, until they were approved and released. A design that did not come from the central library would not have the proper cryptographic signature, and the factory would simply refuse to build it.

Product Design Parameters

Rapid innovation is a key benefit of nanotechnology. The rapid and flexible manufacturing process allows a design to be built and tested almost immediately. Because designers of nano-built products do not have to do any actual nanotech research, a high

level of innovation can be accommodated without giving designers any access to dangerous kinds of products. As mentioned above, a design with billion-atom, sub-micron blocks—permitting specification of near-biological levels of complexity—would still pose no risk of illicit self-replication. The minimum building block size in a design could be restricted by the design system. A fully automated evaluation and approval process could also consider the energy and power contained in the design, its mechanical integrity, and the amount of computer power built in. The block-based design system provides a simple interface to the block-based convergent assembly system. A variety of design systems could be implemented using the same nanofactory hardware, and the designer would not have to become an expert on the process of construction to create buildable designs.

With a safe-design nanofactory, adults—and even children—could safely play with advanced robotics, inventing and constructing almost anything they could imagine. (Today, adults as well as children find it worthwhile to play with the Lego MindStorms™ system[14].) More powerful products would require an engineering certification. This could be given to any responsible adult, since even a malicious product engineer would be unable to bypass the factory's programming and cause it to make illicit fabricators. A product that included chemical or nanomechanical manipulation ability would have to be carefully controlled, even during the design phase, to prevent the designer from building something that could be used for illicit nanomanufacturing.

Risks and dangers associated with products could be assessed on a per-product basis. Many products, produced with simplified design kits, could be approved with only automated analysis of their design. Most others could be approved after a safety and efficacy assessment similar to today's approval processes. Only rarely would a new degree of nanotechnological functionality be required, so each case could be carefully assessed before the functionality was added to appropriately restricted design programs.

Product approval for worldwide availability could depend on any of several factors. First, unless designed with a child-safe design program, it could be evaluated for engineering safety. Second, if the design incorporated intellectual property, the owner of the property could specify licensing terms. Third, local jurisdictional restrictions could be imposed, tagging the file according to where it could and could not be manufactured. Finally, the design would be placed in the global catalog, available for anyone to use.

Conclusion

Nanotechnology offers the ability to build large numbers of products that are incredibly powerful by today's standards. This possibility creates both opportunity and risk. The problem of minimizing the risk is not simple; excessive restriction creates black markets,

which in this context implies unrestricted nanofabrication. Selecting the proper level of restriction is likely to pose a difficult challenge.

This paper describes a system that allows the risk to be dealt with on two separate fronts: control of the nanotech manufacturing capacity, and control of the products. Such a system has many advantages. A well-controlled manufacturing system can be widely deployed, allowing distributed, cheap, high-volume manufacturing of useful products and even a degree of distributed innovation. The range of possible nanotech-built products is almost infinite. Even if allowable products were restricted to a small subset of possible designs, it would still allow an explosion of creativity and functionality.

Preventing a nanofactory from building unapproved products can be done using technologies already in use today. It appears that the nanofactory control structure can be made virtually unbreakable. Product approval, by contrast, depends to some extent on human institutions. With a block-based design system, many products can be assessed for degree of danger without the need for human intervention; this reduces subjectivity and delay, and allows people to focus on the few truly risky designs.

In addition to preventing the creation of unrestricted nanotech manufacturing devices, further regulation will be necessary to preserve the interests of existing commercial and military institutions. For example, the effects of networked computers on intellectual property rights have created concern in several industries[15], and the ability to fabricate anything will surely increase the problem. National security will demand limits on the weapons that can be produced.

Forthcoming papers will give recommendations for a multi-purpose system of administration that preserves commercial rights and security imperatives, while still allowing humanitarian and innovative use.

This paper has outlined a scenario for the safe development and use of advanced nanotechnological manufacturing. Unrestricted nanotech manufacturing creates several high-stakes risks. The use of a restricted nanofactory design that is safe for widespread deployment can mitigate some of these risks, and other risks can be dealt with piecemeal by making many low-stakes decisions about the factory's products. Careful attention must be paid to security during the initial nanofactory development, and wise administration must be implemented to prevent both undesired products and pressure for black markets or independent development. With these caveats, however, the system presented here preserves almost all the benefits of unrestricted nanotechnology while greatly reducing the associated risks.

References

[1] *There's Plenty of Room at the Bottom* is the title of a famous speech given by Richard P. Feynman on December 29, 1959. A transcript can be found at http://www.zyvex.com/nanotech/feynman.html

[2] K. Eric Drexler, *Engines of Creation,* Anchor Press, 1986.

[3] K. Eric Drexler, *Nanosystems: Molecular Machinery, Manufacturing, and Computation,* John Wiley & Sons, 1992.

[4] These fears have already been exploited in popular fiction.

[5] For an analysis of these and other risks, see *Accidents, Malice, Progress, and Other Topics,* at http://www.foresight.org/Updates/Background2.html

[6] The best paper to date on the topic is *Nanotechnology and International Security* by Mark Gubrud. See http://www.foresight.org/Conferences/MNT05/Papers/Gubrud/

[7] Perhaps the leading writer in this area is economist Robin Hanson. A good overview of the potential impact of emerging technologies on the world economy is *What It Takes to Get Explosive Economic Growth,* online at http://www.jetpress.org/volume2/singularity.htm

[8] See, for example, *NANO-ECONOMICS* at http://www.geocities.com/computerresearchassociated/NanoEconomics.htm

[9] *Nanotechnology: the potential for new WMD* http://www.janes.com/security/international_security/news/jcbw/jcbw030115_1_n.shtml

[10] *Forward to the Future: Nanotechnology and Regulatory Policy,* by Glenn Harlan Reynolds, was published in November 2002 by the Pacific Research Institute. It is available online at http://www.pacificresearch.org/pub/sab/techno/forward_to_nanotech.pdf

[11] The authors will analyze these issues in detail in forthcoming papers.

[12] *The Diamond Age*, Neal Stephenson, Bantam Spectra, 1995 (and subsequent publishers)

[13] See *Security Attributes Based Digital Rights Management* at http://www.ub.utwente.nl/webdocs/ctit/1/00000079.pdf

[14] See *LEGO MindStorms*™ at http://mindstorms.lego.com/eng/default.asp

[15] See *Libraries in Today's Digital Age: The Copyright Controversy* at http://ericit.org/digests/EDO-IR-2001-04.shtml