

Computing Naturally: Benefits and Risks of Nanotechnology

by Nicolas Logan & M. E. Kabay, PhD, CISSP-ISSMP
School of Business & Management
Norwich University, Northfield VT

In the last of three brief articles looking at biologically-based or –inspired computing, Norwich senior Nicholas K. Logan, CEH began with a discussion of genetic algorithms and then reviewed DNA-based computation. Today he examines some implications of tiny semi-autonomous, possibly self-replicating machines – artificial organisms constructed and perhaps programmed with tiny components. Everything that follows is Mr Logan’s work with minor edits.

Nanotechnology

DNA origami falls into the realm of building structures with nanometer-sized materials (10^{-9} m), but it is only a basic building block. Nanobots are robots designed at the molecular level, measured in millionths of a meter (nanometers). The development of nanobots is progressing through use of current technologies to produce engines that are operating at the nano-scale. < <http://www.youtube.com/watch?v=S4CjZ-OkGDs> > Nanobots will be able to function within organisms as a part of the system; for example, nanobots could be designed and programmed to work within the human body to perform many functions that the human body requires, but with greater effectiveness and precision than human cells. The nanobots could monitor and replace damaged body parts and interface with digital computers to order replacement nano-material for the host body. For an interesting discussion of the potential of nanobots, see p 28 ff of Kurzweil, R. (2006). *The singularity is near: when humans transcend biology*. Penguin (ISBN 0143037880). 672 pp. AMAZON < <http://www.amazon.com/Singularity-Near-Humans-Transcend-Biology/dp/0143037889> >

Threats from Nanotechnology

The obvious threat of self-replicating nanotechnology is that their cellular structure will allow them to mutate, as a cell does, and with the advanced technology involved in their creation they will become a far more dangerous cancer than any naturally occurring disease. In science-fiction films and series, rogue nanobots are a common theme; for example, in the popular *Stargate SG-1* < <http://stargate.mgm.com/view/series/1/index.html> > and *Stargate Atlantis* < <http://stargate.mgm.com/view/series/2/index.html> > television series, several episodes involve *nanites*, the term the series use for nanobots:

- “Learning Curve” < <http://www.imdb.com/title/tt0709113/> > has nanites that extract information from children and then spread the information throughout society by replication and implantation.
- In “Nemesis” < <http://www.imdb.com/title/tt0709128/> >, *replicators* are self-reproducing nanites that form insect-like ravaging hordes.
- “Small Victories” < <http://www.imdb.com/title/tt0709173/> > continues the story line with destructive replicators that slaughter humans.
- “Enemies” < <http://www.imdb.com/title/tt0709077/> > includes a Replicator-infected ship with no people left on it.

- “Unnatural Selection” < <http://www.imdb.com/title/tt0709214/> > finds an entire galaxy overrun by replicators.
- “New Order: Part 2” < <http://www.imdb.com/title/tt0709131/> > continues the story of the battle against the replicators.
- “Reckoning” parts 1 < <http://www.imdb.com/title/tt0709151/> > and 2 < <http://www.imdb.com/title/tt0709152/> > has replicators adapting themselves into clones of living creatures including key characters in the series.

Dennis E. Shasha and Cathy Lazere point out that the communication of nanobots and digital computers could, “easily turn (a nanobot) into a spy,” and that the faster computers created though natural computation and nanotechnology could be used to produce more effective weapon systems (*Natural Computing: DNA, Quantum Bits, and the Future of Smart Machines* < <http://www.amazon.com/Natural-Computing-Quantum-Future-Machines/dp/0393336832> >, p 235).

If such semi-autonomous, microscopic computers were to spread throughout society, unauthorized nanobot reprogramming or control could lead to serious damage to system that were depending on these devices. One can imagine self-contained nanobots being inserted into a patient to repair a damaged heart – and then being subverted by criminal hackers to destroy heart tissue instead of healing it.

Concluding Remarks

These new technologies may have some serious risks for humanity such as new forms of cancer, technological growth at rates that may surpass human knowledge, spies within our bodies, computers capable of mass destruction, and systems capable of breaking the world’s best ciphers in seconds.

However, these systems may also have significant benefits. Even a virulent cancer forming inside a body might be less damaging than current cancers if nanobots contributed to a more effective immune system; such devices could also help to detect and monitor diseases much earlier. Conceivably, self-replicating semi-autonomous nanobots could cure various degenerative diseases.

The idea that computers might develop beyond human control may be a risk, but these devices could also benefit society. < <http://www.peterhollings.com/?p=272> > For example, code-breaking systems can be used for good (e.g., helping law enforcement) and evil (e.g., helping dictatorships) and will motivate future advancements in cryptography and cryptanalysis.

The destruction of the world has been possible since the development of the hydrogen bomb. So, regardless of how powerful possible computer-made weapon systems are, humanity has already enabled global destruction.

Humanity has always created new technologies and each technology has had its risks. It seems that the more advanced the technological achievements of humanity become the greater the inherent risks of the innovations. Yet, through awareness, control, forethought, and possibly luck humanity is still present in the universe. We have not blown ourselves off the surface of the planet.

The very fact that humanity is aware of the risks posed by the fields of natural computation is the first step in averting these risks and establishing guidelines for research and use of these upcoming technologies. The questions in the end have to be whether humanity is ready to stop advancing because of fear of technologic advancements, whether it is possible to stop innovation, and whether it is wise to stop innovation when others may still be advancing despite our restraint.

* * *

Nicholas K. Logan, CEH is a member of the Norwich University Corps of Cadets. After he graduates with his BSc in Computer Security and Information Assurance in May 2011, he will be working for a large Washington, DC area consulting firm where he has been an intern working on risk management Monte Carlo modeling. He is a member of the Association for Computing Machinery and has been inducted into the Upsilon Pi Epsilon honor society. In addition to his wide interests in information security and risk management, he is fascinated by computational complexity theory, artificial intelligence, and evolutionary theory.

M. E. Kabay, < <mailto:mekabay@gmail.com> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc. < <http://acsi-cybersa.com/> > and Associate Professor of Information Assurance < <http://norwich.edu/academics/business/infoAssurance/index.html> > in the School of Business and Management < <http://norwich.edu/academics/business/faculty.html> > at Norwich University. < <http://www.norwich.edu> > Visit his Website for white papers and course materials. < <http://www.mekabay.com/> >

Please support Norwich University ROTC student Zach Wetzel's fund-raising run for the Semper Fi Injured Marines Fund. < <http://www.active.com/donate/semperfifundmcm2011/fundZWetzel> >

Copyright © 2011 Nicholas K. Logan & M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.