U.S. National Security In New Times

Steven D. Nixon
Formerly of the Office of the Director of National Intelligence

INTRODUCTION

Our national security stands at a critical crossroads. For a generation we confronted the Soviet Union in a Cold War that ended with the collapse of that empire in 1991. Now, seventeen years later, our national security establishment has failed to evolve significantly to confront the new challenges facing the country. Today, religious and ethnic tensions, independence movements, and terrorism have reemerged as major security challenges. However, unlike anytime in history, these challenges are being supercharged by globalization – the rapid advance and spread of technology around the world. This spread of technology is empowering small groups and individuals, leading to new and very dangerous weapons proliferation challenges. A looming example of such a threat involves the rapid advances in biotechnology and the potential for relatively easy creation of new and devastating biology inspired weapons.

To meet the challenges of this age of globalization, we must significantly adapt our national security posture. We can't win by resorting to our traditional focus on bigger satellites, faster fighter aircraft, or quieter submarines that now take decades to deploy for ever increasing withdrawals from the treasury. The bottom line is that we must significantly improve our agility, innovation, and collaboration. Since such characteristics run counter to the usual behavior of large government bureaucracies, we

should seriously consider the option of creating a variety of small agile government agencies while also outsourcing new activities to small agile companies.

WE WON THE COLD WAR, BUT . . .

The end of the Cold War left the United States as sole remaining superpower -- at least for the time being. Our economy is the largest in the world and we enjoy tremendous competitive advantages in technology and many other areas critical to sustaining a leading position in global affairs.

Without a Soviet Union to confront, our national security apparatus thrashed around throughout the 1990s looking for a new raison d'être. Though the September 11, 2001 attacks brought significantly increased focus on terrorism, our security establishment still largely retains the same processes, culture, values, technical capabilities, and organization originally developed to confront the Soviets. And so we face the classic position of a successful enterprise that is ironically handicapped by its own prior success. The National Academy, in a study entitled "Rising Above the Gathering Storm" stated,

> "There can be no more dangerous place to be than in first place: the one holding that exalted position becomes everyone else's target, and perhaps worse, is the recognized beneficiary of the status quo – and therefore reluctant to promote, or even accept, change."

Such a situation makes us extremely vulnerable to disruptive changes in the global security environment. Great companies face this problem all the time and either

successfully adapt or go out of business. Clayton Christianson, famous for his study of disruptive technologies, writes

> "They [industry leaders] pour resources into their core business. They listen to their best customers. And in doing so, industry leaders get blindsided by disruptive innovations—new products, services, or business models that initially target small, seemingly unprofitable customer segments, but eventually evolve to take over the marketplace. This is the innovator's dilemma—and no company or industry is immune." (Christianson and Raynor, 2003)

While the current and future security environment demands greater agility from our national security establishment, we have moved in just the opposite direction. For example, the first Corona optical spy satellite took just over 2 years from start to first successful launch. It is not at all unusual for new government satellite programs today to require over a decade to achieve first launch. And while we now measure our innovation cycle times in decades, our adversaries like the insurgents in Iraq, measure theirs in weeks. The *Washington Post* reported last year,

> "The Improvised Explosive Device struggle has become a test of national agility for a lumbering military-industrial complex fashioned during the Cold War to confront an even more lumbering Soviet system.
>
> 'If we ever want to kneecap al-Qaeda, just get them to adopt our procurement system. It will bring them to their knees within a week,' a former Pentagon official said." (Atkinson, 2007)

FROM THE COLD WAR TO GLOBALIZATION – AN INFLECTION POINT FOR NATIONAL SECURITY

Andy Groves, the former CEO of Intel, describes the onset of strategic inflection points as that point in which a business transitions from the old state of affairs to a new. These states are often brought about by what he calls "10x" changes in one or more of the key forces that impact a business.

The world has seen many "10x" changes since the end of the Cold War. Nowhere is this clearer than in the area of technology in which observed trends in accelerating advances are now described as "laws." The most famous such law is undoubtedly "Moore's Law" which states that the number of transistors that can be placed inexpensively on a integrated circuit doubles every 2 years. Moore's Law has now inspired a cottage industry of sorts with a proliferation of technology "laws":

- Disk storage density doubles every 12 months (Kryder's Law)
- Bandwidth to high-end home users doubles every 21 months (Nielsen's Law)
- Amount of data coming out of an optical fiber doubles every nine months (Butter's Law)
- Amount of available DNA sequence data doubles every 18 months (observed, but awaiting someone to attach name) (Bio Economic Research Associates, 2007)

The United States no longer corners the market in technology, in fact we are now a net importer of technology products, and these advances are now available globally. (National Science Foundation, 2008) Such trends inspired Thomas Friedman to write the

bestseller “The World Is Flat” which asserts that the diffusion of accelerating technical advances around the globe is creating the ultimate level playing field. (Friedman, 2005)

Our friends and adversaries from around the world now have access to the same powerful technical capabilities. Enabled with these new capabilities, small groups and individuals now have the wherewithal to threaten event the mightiest of nations. Consider the impact of 19 men on September 11th using modern aviation technology against us. They not only killed thousands of Americans, but also drove our country to spend nearly $1 trillion in response. The amount spent on the Iraq and Afghanistan wars already exceeds the amount spent on Viet Nam, even when adjusting for inflation. (Stiglitz and Bilmes, 2008)

Though our national security operations are running at an exceedingly high tempo, it is my experience that the government transformation needed to face the “Flat World” is near paralysis. In some sense, this is understandable. Andy Groves describes this condition as companies face strategic inflection points:

> “Ideas about the right direction will split people on the same team. After a while, everyone will understand that the stakes are enormously high. There will be a growing ferocity, determination and seriousness surrounding the views the various participants hold. People will dig in. These divergent views will be held equally strongly, almost like religious tenets. In a workplace that used to function collegially and constructively, holy wars will erupt, pitting coworkers against coworkers, long-term friends against long-term friends. Everything senior management is supposed to do – define direction, set strategies, encourage team

work, motivate employees – all these things become harder, almost impossible. Everything middle management is supposed to do – implement policy, deal with customers, train employees – also becomes more difficult." (Groves, 1999)

TRENDS IN BIOTECHNOLOGY – SOON ALMOST ANYONE CAN HAVE A WEAPON OF MASS DESTRUCTION

A great example of the potential threat from globalization is the proliferation of biotechnology that could allow almost anyone with minimal technical savvy to build some pretty scary bio capabilities. DNA sequencing capabilities are proceeding faster than Moore's law (Bio Economic Research Associates, 2007). Nasty viruses such as polio and Spanish flu have not only been sequenced, but have also been artificially reconstructed directly from these sequences. (Cello *et al.*, 2002) (Taubenberger et al 2005). The National Institute of Health recently reported,

> ". . . considering the rapid development of molecular biology, it is only a question of time before the artificial synthesis of agents or new combinations of agents becomes possible. This danger was highlighted last year by a worrying article in *Science*: a research team at the State University of New York in Stony Brook chemically synthesized an artificial polio virus from scratch (Cello *et al.*, 2002). They started with the genetic sequence of the agent, which is available online, ordered small, tailor-made DNA sequences and combined them to reconstruct the complete viral genome. In a final step, the synthesized DNA was brought to life by adding a chemical cocktail that initiated the production of a living, pathogenic virus. (National Institute of Health, 2008)

Today, websites such as www.mrgene.com offer online DNA synthesis – just

submit your sequence to the website, and they will quickly ship your gene. Incidentally, they happen to be running a special in June and July 2008 – your gene sequence for just $0.49 per base pair! (www.mrgene.com, 2008) Wired recently reported that "Scientists Build First Man-Made Genome; Synthetic Life Comes Next" (Madrigal, 2008)

If the prospect of bioterrorism sounds far fetched, consider that there is in fact a long sad history of such attacks; bioterrorism dates as far back as ancient Roman civilization where dead and rotting animals were thrown into wells to poison water supplies (http://en.wikipedia.org/wiki/Bioterrorism). Though the anthrax attacks immediately following September 11 represent a recent example in the United States, prior to that the Rajneeshee bioterror attack of 1984 sickened 750 individuals in Oregon with salmonella food poisoning (http://en.wikipedia.org/wiki/1984_Rajneeshee_bioterror_attack)

Given current advances in technology, it is not too hard to imagine a world a few years from now in which a teenager can create a biological virus almost as easily as today's teenager can create a computer virus. This is indeed a scary future.

CONCLUSION

How will the national security establishment respond to this threat and others that derive from current technology trends (cyber attack comes to mind)? Advantage now goes to the organizations that can operate faster, more innovatively, and more collaboratively. In my last job as Director of Science and Technology for the Director of National Intelligence, we called this "Speed, Surprise, and Synergy." Similarly Secretary of Defense Robert Gates, in a recent speech, said "But these new threats also

require our government to operate as a whole differently – to act with *unity, agility, and creativity*." (Gates, 2007)

We must recognize that we no longer live in the industrial age, and traditional industrial scale solutions simply cannot in themselves address many of our current problems. The information age is further evolving into a new networking age in which everyone and everything is connected. Our national security establishment must learn to operate across interlinked social networks, financial networks, communication networks, and computer networks. We must make decisions, produce capabilities, and operate at network speed, not industrial speed. Our national security establishment's love affair with hard science, particularly physics, chemistry, and engineering must share more time with other sciences like biology, anthropology, and psychology. The US Government must learn to work more effectively with non-government providers and our allies. Further, we should create small, agile, innovative agencies and also outsource more activities to small, agile innovative companies that have an easier time avoiding crippling bureaucratic barriers. In short, we must let go of the Cold War way of doing things, and move boldly into the 21st century.

REFERENCES

Atkinson, Rick. 2007. The Single Most Effective Weapon Against Our Deployed Troops. Washington Post . Sep 30, 2007. Page A1.

Bio Economic Research Associates. 2007. Genome Synthesis and Design Futures: Implications for the US Economy. http://www.bio-era.net/research/GenomePurchaseForm.html,

Cello, J., Paul, A.V., Wimmer, E. 2002. Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. Science. 297. 1016–1018.

Christianson, C., Raynor, M. 2003. Innovator's Solution: Creating and Sustaining Successful Growth. Harvard Business School Press.

Friedman, Thomas. 2005. The World is Flat: A Brief History of the Twenty-First Century. Farrar, Straus and Giroux. New York.

Gates, Robert. 2007. Landon Lecture (Kansas State University). Remarks as Delivered by Secretary of Defense Robert M. Gates, Manhattan, Kansas, Monday, November 26, 2007

Groves, Andy. 1999. Only the Paranoid Survive. Doubleday. New York.

Madrigal, Alexis. 2008. Scientists Build First Man-Made Genome; Synthetic Life Comes Next. Wired Magazine. January 24, 2008.

National Academy of Science. 2007. Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future. National Academies Press. http://www.nap.edu/catalog.php?record_id=11463

National Science Foundation, 2008. Chart: "U.S. trade balance in high-technology goods: 2000–06. http://www.nsf.gov/statistics/seind08/slides.htm

Stiglitz, J., Bilmes L., 2008. The Three Trillion Dollar War. The Times. February 23, 2008.

Taubenberger, J. K., Reid, A., Laurens, R.M., Wang, R., Jin, G., Fanning, T. G. 2005. Characterization of the 1918 Influenza Virus Polymerase Genes. Nature. 437. 889–893. October 6, 2005.

Van Akin, J., Hammon, E. 2003. Genetic engineering and biological weapons. European Molecular Biology Organization. Summarized at http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1326447

Zachary, G. P. 2007. When the Military Needs it Yesterday. New York Times. October 21, 2007.