Converging Technologies: The Future of the Global Information Society (RSA Information Security Award for Outstanding Achievement in Government Policy, 2004)

Conference Paper · December 2002

CITATIONS
3

READS
71

CONVERGING TECHNOLOGIES:

THE FUTURE OF THE GLOBAL INFORMATION SOCIETY

Christopher Altman

Chairman
First Committee on Disarmament and International Security
United Nations International Student Conference Amsterdam

TABLE OF CONTENTS

The UNISCA First Committee chair briefing, *"Converging Technologies: The Future of the Global Information Society*," was recently selected as recipient of the RSA Award for Outstanding Achievement in Government Policy.

The RSA Conference and Awards is the "world's most prestigious international information security conference for organizations that deploy, develop or investigate security or cryptography."

Previous RSA Keynote speakers and RSA Awards recipients include **Bill Gates**, Microsoft Corporation, US Congressman **Tom Davis**, and **Richard Clarke**, former White House Security Advisor.

. . . . . .

Converging Technologies : The Future of the Global Information Society

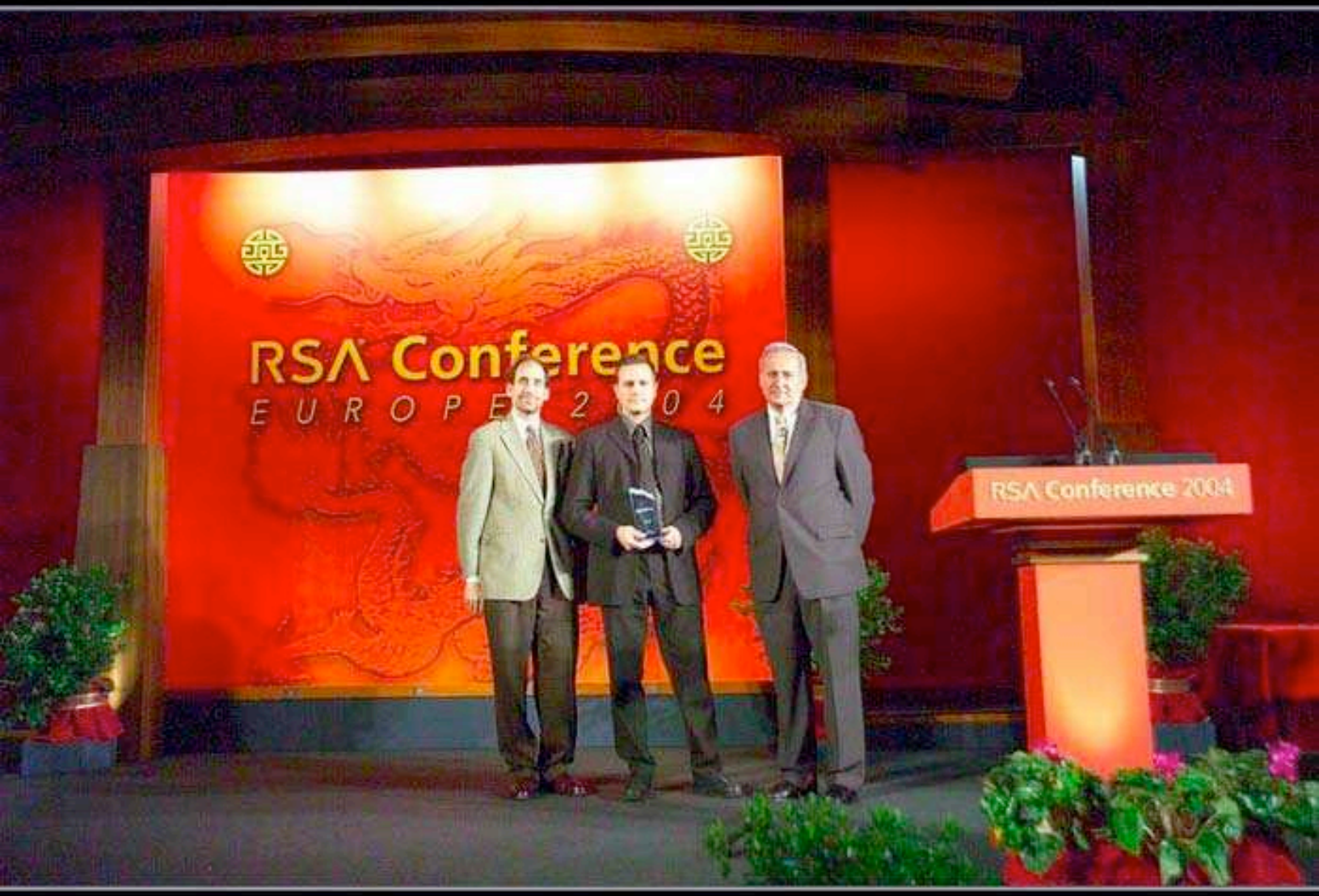
Christopher Altman
Chairman, First Committee on Disarmament and International Security

http://infosec.casimirinstitute.net/convergence.pdf

Abstract.

The complex web of the global information grid will undergo explosive changes over coming decades. As advances in science and technology converge, a myriad array of discoveries in biotechnology, nanotechnology and information technology will produce unpredictable effects that must be accounted for in any estimate of what the world will look like in this future.

A strategically important feature of this world will be the emerging trend of information warfare. Though still immature at present day, this trend will become increasingly dominant in the years to come. The information warfare of tomorrow will be radically different from its prototype today. No longer will it be confined to the mainframes of the Internet or to corporate databases: the battleground of the future will draw into its scope the scientific advances being made today in bio- and nanotechnologies. Divisions between man and machine will blur – when networked technologies are ubiquitous, a state-sponsored attack on electronic networks can have far-reaching – and devastating – physical consequences.



2004 RSA Information Security Award
Outstanding Achievement in Government Policy

22 December 2002

> I believe that we are at the most critical place and time in human history. Indeed, these are the times and we are the people who must act. If not now, then when? If not you, who? What we do makes a profound difference.
>
> Jean Houston

The sixth annual UNISCA conference was a resounding success. I am extremely proud of the extraordinary commitment that the delegates displayed – with their maturity, their dedication, and with the extraordinary efforts that they put forward into making the week such a success.

Active involvement and cooperation are essential for bringing about a better tomorrow. No one is unaffected by the events occurring in the world today – we are all interconnected, and we are all interdependent upon one another to create a better world.

By taking part in UNISCA, each one of us has taken the important step of working towards a solution for the myriad challenges our world faces today. Our actions can serve as a positive force and as an instrument of change to make our world a better place. I am deeply honored to be working with so many others who share this long-term vision for humanity.

Sincerely,

Christopher Altman*
Chairman, First Committee

* Home: http://infosec.casimirinstitute.net/
Contact: altman@casimirinstitute.net

CONVERGING TECHNOLOGIES:

THE FUTURE OF THE GLOBAL INFORMATION SOCIETY

Christopher Altman

First Committee on Disarmament and International Security

There are but two powers in the world: the sword and the mind.
In the long run, the sword is always beaten by the mind.

Napoleon Bonaparte

The antithesis of security is complexity.

Jim Hughes, INFOSEC

Introduction

The complex web of the global information grid will undergo explosive changes over the coming decades. As advances in science and technology converge, a myriad array of discoveries in biotechnology, nanotechnology and information technology will produce unpredictable effects that must be accounted for in any estimate of what the world will look like in this future. A strategically important feature of this world will be the emerging trend of information warfare. Though still immature at present day, this trend will become increasingly dominant in the years to come.

The information warfare of tomorrow will be radically different from its prototype today. No longer will it be confined to the mainframes of the Internet or to corporate databases: the battleground of the future will draw into its scope the scientific advances being made today in *bio*- and *nano*- technologies. The divisions between man and machine will blur.

When networked technologies are ubiquitous, a state-sponsored attack on the Internet can have far-reaching, and devastating, physical consequences. This briefing examines the contributing factors that have lead to shaping this most unique of times in human history. Alvin and Heidi Toffler's *Third Wave* has been realized. We live in an increasingly information-dominated world, vulnerable to attack from the very features that give it its power and versatility. In digital space, location no longer bears any meaning.

Convergence

Futurists Alvin and Heidi Toffler mapped the evolution of society in three progressive 'waves': the agrarian, industrial, and information stages of development. These transitions revolutionized the very foundations of modern society. We are now witnessing the convergence of technologies catalyzed by the information age. We have traversed the crest of the Third Wave, and will witness in the 21st century a synthesis of knowledge that can only be characterized as a new Renaissance.

The Third Wave transition was roughly concurrent to the advent of the networked computer. ARPANET, the predecessor to the modern Internet, was developed by the US Advanced Research Projects Agency to facilitate communications between government and university researchers. But the scientists who developed this network had no way to foresee how quickly the Internet would grow to encompass the world. Its rapid explosion into the worldwide web marked a phase transition of unprecedented proportions – one that has propelled the world headlong into the age of networked information.

The sweeping changes brought about by the information revolution have sent resounding shockwaves through society, transforming virtually every field of scientific endeavor. But driven by Moore's Law, these changes are only accelerating in their progression. The Internet will change beyond recognition over the coming decades. Optical routing will bring increased bandwidth. Embedded micro-electromechanical sensors, no larger than a

grain of sand, will link appliances together through wireless communications. The network will become a truly ubiquitous medium. These advances alone would deeply transform the world around us. But the field of information technology does not exist in a vacuum – the revolution in informatics is inextricably linked to every other field of scientific inquiry.

> Our machines will become much more like us, and we will become much more like our machines.
>
> Rodney Brooks

Synergistic advances in neuroscience and artificial intelligence will profoundly change the way we look at ourselves and the world around us. When asked what to expect from science over the coming years, an interdisciplinary committee of Nobel laureates[1] agreed upon one thing: the coming years will bring revolutionary changes in our understanding of the mind. Dr. Ronald Brachman, Director of the DARPA Information Processing Technology Office, has gone so far as to say that "we will move from the age of information to the age of cognition[2]."

An omni-linked world populated with intelligent artifacts will bring sweeping changes to virtually every facet of modern life – from science and education to industry and commerce – leaving no segment of society unaffected by its advance. How will civilization change in response to a world saturated with embedded intelligence? How can these technologies be best applied to improve the human condition? These issues will become increasingly important as advances in science and technology bring us closer to unveiling the mysteries of the mind.

Biotechnology and information technology will continue to drive each other in a synergetic interplay of discovery. Medicine has been one of the greatest beneficiaries of

[1] BBC News, *Nobel Minds*. 15 December 2002.
[2] Defense Advanced Research Projects Agency. *Systems that Know What They're Doing.*

the information age, as increasing computational power drives innovation and facilitates the discovery of new therapies. Bioinformatics will transform health care and increase our resistance to disease. Debates over privacy and the control of information will become forefront issues. Who owns the information contained in your DNA? Rapid advances in genome sequencing, drug prototyping, and even eugenics will pose controversial and difficult questions to society in the years to come.

> If I were asked for an area of science and engineering that will most likely produce the breakthroughs of tomorrow, I would point to nanoscale science and engineering[3].

Materials technology is yet another beneficiary of the Third Wave revolution. Technologies such as rapid prototyping and self-assembly will change the nature of manufacturing. Advanced polymers allow for the creation of highly versatile and robust industrial products. Adaptive materials will sense and respond to changes in their environment.

Perhaps the greatest of possibilities lies within the domain of nanotechnology – the science of manipulating matter at its smallest scales. A society with the capability to harness advanced nanotechnologies in the form of molecular manufacturing is the information society fully realized – a society that has taken the knowledge gained from the information revolution, and directly channeled it to inject that information back into the environment. As envisioned, nanotechnology in effect transforms matter into software: if an idea can be imagined within the bounds of physics, it can be transferred into matter. In this case, atoms themselves are the building blocks of manufacture.

> Never has such a comprehensive technology promised to change so much so fast. Inevitably, nanotechnology will give people more time, more value for less cost, and provide for a higher quality of existence. Those nations, governments, organizations and citizens who are unaware of this impending power shift must be informed and enabled so that they may adequately adapt[4].

[3] Neal Lance, Former Science and Technology Advisor to the President of the United States
[4] James Canton, President, Institute for Global Futures

The convergence of these technologies has reaped innumerable benefits to our quality of life, and brought about a dramatic rise in innovation. But the Third Wave transition has been an unevenly distributed phenomenon. For the first time in history, agrarian and industrial economies share borders with those that have already successfully navigated the transition to becoming information societies. This imbalance brings tension, and it sets the stage for future conflict. If we cannot properly channel our technologies to eliminate our political, economic and social backwaters, we will see further instability and reduced security around the globe. In an age of ubiquitous technology and relative prosperity, this condition is simply not acceptable.

Conflict

> Information age technology is making the environment in which future military operations occur more dynamic and unpredictable. It renders national economies sensitive to global developments, heightens cultural and political awareness on the part of the world's populations, and fuels radical movements that promote worldwide political fragmentation and destabilization[5] .

How will continuing technological advances interface with information warfare? The conflicts of tomorrow will know no borders. The lines of demarcation between organic and synthetic will begin to blur – the network of the future will behave more like a living organism than a digital computer. The pervasiveness of technology will require security measures that are robust, versatile and adaptable to changing conditions.

> The electron, in my view, is the ultimate precision-guided weapon.
>
> John Deutch, Former DCI

[5] Echevarria 30.

In its broadest sense, information warfare has existed since the advent of human communication and conflict. But the dawn of the Third Wave society has brought us to the point where information has become the dominant medium of exchange that drives the global economy. Our societal dependence upon these technologies makes us increasingly vulnerable to attack from the digital arena.

Present-day infrastructures are perilously unprepared for this kind of attack. Future strategic contingencies must deem national preparedness to be of critical importance. Former CIA Director John Deutch ranks the threat of information warfare as a 'close third' behind the threat from weapons of mass destruction and the proliferation and terrorist use of nuclear, biological and chemical weapons[6]. But the nature of this threat is difficult to define. With no traditional battlefield, no borders, and no clearly defined combatants, securing our digital infrastructures seems an impossible task.

> The day may well come when more soldiers carry computers than carry guns.
>
> Alvin and Heidi Toffler

Conventionally, information warfare has been viewed through the lens of conventional warfare: 'surgical' strikes to eliminate infrastructure centers, communications posts, and sensor arrays – all have focused on waging war as a zero-sum game. But the nature of information itself changes the fundamentals of how this kind of war must be waged.

This point has not gone unnoticed: the military has already set its sights upon the next generation of conflict. Traditional strategic models will soon be superceded through the next generation of enabling technologies. The USAF 2025 Final Report calls for mature

[6] Joyner and Lotrointe 2001.

and highly sophisticated global strike capability, using an array of advanced technologies including mini-satellites, microsensors and holographic projection systems. The network would extend traditional military capabilities to encompass information attack, deception, biomedical attack, and multispectral warfare[7]. This change marks a radical departure from present-day military options, fueled by the very technologies that are driving the information revolution.

> The most sophisticated and important information warfare 'battles' of the future may be waged with adversaries who never know they were 'defeated[8].'

By definition, the most successfully waged information campaigns are never made public. Information warfare is ultimately about shaping minds: it is about changing ideas and perceptions. A Third Wave society is especially sensitive to this kind of manipulation. In a society dominated by information exchange, 'reality' is malleable. Opinions can sway in response to information presented by government, media, industry and outside influences. Information, and *dis*information, become powerful weapons – applied memetic engineering. The virtual world of the internet allows unprecedented freedom of movement along this axis. Spheres of influence become location independent. The mind is both the currency of the net and the battleground of the future.

> Warfare is about achieving behavioral change, and the highest art is to accomplish that change without a single shot being fired.
>
> John L Peterson

[7] USAF2025
[8] Peterson 2000.

Complexity

> I think the next century will be the century of complexity.
>
> Stephen Hawking

Future strategic initiatives must shift from traditional, Newtonian modes of thinking in order to harness the emergent complexity and parallel processing capabilities of fully networked information systems. In systems that extend orders of magnitude beyond the limits of understanding, the very concept of *control* must undergo a fundamental redefinition. Complex systems theory offers an array of promising techniques to aid tactical analysis in this area.

> I shall proceed from the simple to the complex. But in war more than in any other subject we must begin by looking at the nature of the whole; for here more than elsewhere the part and the whole must always be thought of together.
>
> Carl van Clausewitz

The Internet is a classical example of the complex dynamical system: it is decentralized, made up of independent autonomous agents, and its structure follows a scale-free topology – a fractal power-law distribution curve. The application of a systems approach[9] to information warfare offers an extended range of options for averting and resolving conflict. Instead of placing focus upon brute force countermeasures, a strategic emphasis on global phase space[10] dynamics encourages proactive thinking – the latter is less costly and less risky, both politically and militarily.

[9] Ilachinski, Peterson, Schneider.

[10] *Phase space:* a mathematical visualization space that describes the behavioral parameters of a dynamical system.

> Whereas conventional wisdom sees combat as essentially a head-on collision between two massive, and perhaps slightly malleable, billiards, obeying a Newtonian-physics-like calculus of interaction, the complex adaptive systems approach sees a self-organizing hierarchy of evolving activity of two interacting 'fluids,' in which global patterns of combat emerge out of an evolving substrate of low-level interaction rules[11].

One potential application lies in the utilization of phase space reconstruction techniques from the field of nonlinear dynamics to reconstruct attractors[12] from real-world data and make short-term behavioral predictions based on underlying patterns[13]. In complex adaptive systems such as the Internet, this feature can play a role in influencing strategic planning in situations where multiple potential paths converge to culminate in a desired outcome.

> It is likely that more and more, InfoTech and InfoWar will be drawn into proactive, preventative roles and missions, designed to assure that some failing or weak part of the system is 'tuned,' resulting in a larger system that is healthier[14].

A related technique offered by a complex systems approach is *chaotic control*, a paradoxical property of chaotic systems in which decision makers can selectively adjust feedback to 'guide' the system into a desired state. Its advantage lies in the fact that it can be applied using only experimental data in which no model is available for the system. Potential applications for chaotic control include selective computer viruses and artificial immune systems. Using advanced visualization techniques[15], genetic algorithms and neural network classifiers, next-generation information warfare theorists may think not in terms of classical warfare, but in the language of complexity.

---

[11] Ilachinski, Part I, p. 19.
[12] *Attractor:* a region of phase space that a system inevitably approaches as it evolves.
[13] Ilachinski, Part II, p. 8
[14] Peterson 2000.
[15] Advanced visualization techniques are being developed at research centers such as Pacific Northwest National Laboratory and under sponsorship of national initiatives under DARPA.

Synergies with developing technologies will bring radical changes to network security as silicon-based networks grow increasingly similar to their biological counterparts, drawing from the principles of Nature itself. Neural networks mimic the behavior of the human brain to classify data and perform pattern recognition. Genetic algorithms apply the principles of chromosomes and mutation to 'evolve' solutions with minimal human intervention, often arriving at results equal or better to their human-designed equivalents[16]. These techniques are not limited to the virtual world; neural network modules can be evolved *directly* into hardware using reconfigurable microchips[17].

> Future networks will not be built, they will be *grown*.[18]

Another model under study to protect future networks is the biological immune system. Artificial immune systems mimic the response characteristics of their biological counterparts, recognizing foreign 'antigens[19]' and mounting an immune response using 'antibodies' to neutralize the threat as it unfolds. Hundley and Anderson define three shared attributes between the biological immune system and the Internet[20]:

> Higher-level biological organisms are comprised of a large number of diverse, complex, highly interdependent components. So is cyberspace.
>
> Biological organisms face diverse dangers that cannot always be described in detail before an individual attack occurs, and which evolve over time. Organisms cannot defend against these dangers by 'disconnecting' from their environment. The same is true of information systems exposed to threats in cyberspace.
>
> Biological organisms employ a variety of complementary defense mechanisms, including both barrier defense strategies involving the skin and cell membranes, and active defense strategies that sense the presence of outsiders, i.e. antigens, and respond with circulating killers, i.e. antibodies.

[16] Brooks, Koza.
[17] Field programmable gate arrays.
[18] Author.
[19] *Antigen*: a foreign protein.
[20] Hundley and Anderson p. 243

Early examples of this technology were developed and deployed at the EU based *Starlab* research laboratory to protect against intruders both physical and digital. Corporate and government research centers across the globe are at work upon similar, biologically inspired techniques to enhance existing network security measures[21]. It is only a matter of time before sophisticated attackers begin to utilize these techniques offensively, placing any system not similarly equipped at a disadvantage in event of an orchestrated attack.

Discussion

> Our machines that function in this environment are like the early biplanes compared to the 747 or the B-2, and our mastery of this environment is akin to our mastery of the air in the 1920s.
>
> Dan Kuehl

There is no doubt that novel technologies will have far-reaching and revolutionary impact on the way we live our everyday lives. Intelligent agents to maximize work productivity, expert systems to analyze massive amounts of data, even household robots to complete tasks and provide companionship and interaction are but a few of the applications that are already invading the marketplace. Commerce and industry, already reliant upon the Internet, will fund new technologies out of a necessity driven by fierce competition in the global marketplace. Self-repairing systems and artificial immune systems will protect critical data servers. Intelligent agents will guide financial transactions. Expert systems will monitor stock market conditions. Decreasing costs and industry competition will spur the onset of an era in which our digital counterparts hold increasing importance in our everyday lives.

[21] Williamson 2002.

The constraints of augmented reality are limited only to our imagination. The physical world will no longer hold its monopoly on experience. Realistic sensory interfaces will be the last hurdle in creating a fully-convincing virtual reality experience. Computers will transmit data not only in the form of the familiar visual and auditory information, but also in the form of tactile and olfactory stimulation. Sensory input will be refined through advances in nanotechnology, with sensors only nanometers across, in some cases directly interfacing with the nervous system. The boundaries between the virtual and the physical world will begin to blur beyond distinction.

How will threats to the global infrastructure be dealt with in this age of rapid change? The threat of information warfare transcends all boundaries. Unconstrained by national borders, the United Nations can work with other international standards bodies to ensure a smooth transition into this age of information. Law enforcement and intelligence agencies, research centers and transnational corporations, national, state and local governments will all have a role to play in assuring the security of information in the universal networked society.

To suggest these changes will come without conflict is naïve; but to suggest halting their development is equally unrealistic. To no small degree, these advances will pose unique ethical dilemmas. Future technologies have the power to transform civilization into potential utopia – or dystopia – depending on society's ability to confront the questions with maturity and tolerance. For the first time in human history, we will truly have the power to harness the engines that drive evolution.

References

Abelson, Hal, Gerald Jay Sussman, Thomas F Knight, Jr., and Radhika Nagpal. *Amorphous and Cellular Computing*. MIT Artificial Intelligence Laboratory 2002.

Albert, Reka, Hawoong Jeong and Albert-Laszlo Barabasi. *Error and Attack Tolerance of Complex Networks.* Nature 406, *pp.* 378-382, 2000.

Alexander, Jane. *BioFutures at DARPA*. Conference Presentation, DARPA Focus 2000. December 2002.

Altman, Christopher. *2001 World Technology Summit*. Conference proceedings, July 2001.

Altman, Christopher. *French Senate Hearing on the Future of Artificial Intelligence*. Conference proceedings, June 2001.

Anderson, Robert H *et al. The Global Course of the Information Revolution: Technological Trends. Proceedings of an International Conference.* National Security Research Division. RAND CF-157-NIC 2000.

Anderson, Robert H, Richard Brackney and Thomas Bozek. *Advanced Network Defense Research: Proceedings of a Workshop*. RAND 2000.

Anton, Philip, Richard Silberglitt and James Schneider. *The Global Technology Revolution: Bio / Nano / Materials Trends and Their Synergies with Information Technology by 2015*. RAND Corporation report prepared for the National Intelligence Council 2001.

Arquilla, John and David Ronfeldt. *Cyberwar is Coming*. RAND 1993.

Arquilla, John and David Ronfeldt. *The Advent of Netwar.* RAND 1996.

Barabasi, Albert-Laszlo. *The Physics of the Web*. PhysicsWeb July 2001.

Brooks, Rodney. *Flesh and Machines: How Robots Will Change Us*. Pantheon Books 2002.

Brooks, Rodney. *Living Machines*. MIT Artificial Intelligence Laboratory 2002.

Carlin, John. *A Farewell to Arms*. Wired Magazine, May 1997.

Crowell, William P. *Information Security in a Third Wave Society*. National Information Systems Security Conference, October 1996.

Defense Advanced Research Projects Agency. *Augmented Cognition: Building Cognitively Aware Computational Systems*. DARPATech 2002 Conference. 31 July 2002.

Defense Advanced Research Projects Agency. *Brain Machine Interfaces*. Hyperlink: www.darpa.mil/dso/. December 2002.

Defense Advanced Research Projects Agency. *Software Programs for Robotic Autonomy*. DARPATech 2002 Conference. 31 July 2002.

Defense Advanced Research Projects Agency. *Systems that Know What They're Doing: The New DARPA/IPTO Initiative in Cognitive Systems.* DARPATech 2002 Conference. 31 July 2002.

Defense Advanced Research Projects Agency. *Technology Transition*. December 2002.

Devost, Matthew G, Brian K Houghton and Neal A Pollard. *Information Terrorism: Can You Trust Your Toaster?* The Terrorism Research Center. December 2002.

Echevarria, Antulio III. *Dynamic Interdimensionality: A Revolution in Military Theory.* Joint Forces Quarterly, Spring 1997.

Erikkson, Anders E. *Information Warfare: Hype or Reality?* The Nonproliferation Review, Spring-Summer 1999.

Gentry, John A. *Doomed to Fail: America's Blind Faith in Military Technology*. Parameters Journal, Winter 2002-2003.

Gonsalves, Paul, *et al. Intelligent Threat Assessment Processor using Genetic Algorithms and Fuzzy Logic.* Charles River Analytics. Proceedings of the 3rd International Conference on Information Fusion, Paris, France. July 2000.

Hundley, Richard O and Anderson, Robert H. *Emerging Challenge: Security and Safety in Cyberspace.* Ch. 10, *Athena's Camp: Preparing for Conflict in the Information Age.* RAND 1997.

Hundley, Richard O *et al. The Global Course of the Information Revolution: Political, Economic and Social Consequences. Proceedings of an International Conference.* National Defense Research Institute. RAND CF-154-NIC 2000.

Ilachinski, Andrew. *Land Warfare and Complexity: An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare*. Center for Naval Analysis, July 1996.

Jablonsky, David. *The State of the National Security State.* Parameters Journal, Winter 2002-2003.

Johnson, L Scott. *A Major Intelligence Challenge: Toward a Functional Model of Information* Warfare. Studies in Intelligence Vol. 01 No. 1, 1997.

Joy, Bill. *Why the Future Doesn't Need Us*. Wired Magazine, April 2000.

Joyner C. and Lotrointe C. *Information Warfare as International Coercion: Elements of a Legal Framework.* European Journal of International Law, Vol. 12 No. 5, pp. 825-866. 2001.

Koza, John. *Concept Formation and Decision Tree Induction Using the Genetic Programming Paradigm*. Stanford University Computer Science Department 1990.

Kuehl, Dan. *Strategic Information Warfare: A Concept*. School of Information Warfare and Strategy, National Defense University, February 1999.

Mees, A. *Chaos in Feedback Systems*. In *Chaos*, edited by Arun V. Holden. Princeton University Press 1986.

Minihan, Lt. Gen. Kenneth A. *Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment*. U.S. Foreign Policy Agenda. USIA Electronic Journal, Vol. 3, No. 4, November 1998.

MITRE. *Current AI Projects*. MITRE Artificial Intelligence Center. Hyperlink: www.mitre.org/resources/centers/ai/curproj.html. December 2002.

MITRE. *Information Warfare: Security for Computer Systems and Databases*. Web article. Hyperlink: www.mitre.org/pubs/showcase/info_warfare2.html. December 2002.

Nagpal, Radhika and Sussman, Gerald Jay. *Robust Engineering Using Biologically-Inspired Models of Cell Differentiation and Morphogenesis.* MIT Artificial Intelligence Laboratory 2002.

National Intelligence Council. *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts.* December 2000.

National Security Agency. *Information Assurance Directorate: Delivering IA Solutions for Cyber Systems.* Hyperlink: www.nsa.gov/isso/brochure/index.htm. December 2002.

National Security Agency. *The National Security Agency: 50 Years of Cryptographic Excellence: Yesterday, Today, and Tomorrow.* NSA 533728. December 2002.

Nichols, Maj. David and Major Todor Tagarev. *What Does Chaos Theory Mean for Warfare?* Aerospace Power Journal, Fall 1994.

Peterson, John L. *Information Warfare: The Future*. Arlington Insitute 2000.

Regis, Ed. *BioWar.* Wired Magazine, November 1996.

Saperstein, Alvin M. *War and Chaos*. American Scientist, November 1995.

Schneider, James J. *Black Lights: Chaos, Complexity, and the Promise of Information Warfare*. Joint Forces Quarterly, Spring 1997.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. Electronic Edition. Thunders Mouth Press 1994.

Smith, George. *An Electronic Pearl Harbor? Not Likely.* Issues in Science and Technology, Fall 1998.

Smith, George. *Truth is the First Casualty of Cyberwar*. Wall Street Journal, 8 September 1998.

Stein, George J. *Information Attack: Information Warfare in 2025*. Air Force 2025 Conference, June 1996.

Toffler, Albert and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*. Little, Brown and Company 1993.

United Nations. *Developments in the Field of Information and Telecommunications in the Context of International Security*. UN General Assembly Resolution 57/53, 2002.

United States Air Force. *Air Force 2025: Final Report*. USAF Air University 1996.

United States Commission on National Security: 21st Century. *New World Coming: American Security in the 21st Century. Major Themes and Implications*. 15 September 1999.

Valverde S, Cancho R Ferrer and Sole R V. *Scale-Free Networks from Optimal Design*. Santa Fe Institute 2002.
Wheeler, Richard. *Artificial Immune Systems and Immune Networks*. Starlab NV/SA 2000.

Williamson, Matthew M. *Biologically Inspired Approaches to Computer Security*. Information Infrastructure Laboratory, HP Laboratories Bristol. 12 June 2002.

Wishner, Richard P. *The Information Fusion Challenge*. DARPATech 2002 Conference. 31 July 2002.

Wood, Lt. Col. Robert J. *Information Engineering: The Foundation of Information Warfare*. Air University 1995.

Wuchty, Stefan and Peter F Stadler. *Centers of Complex Networks*. Santa Fe Institute 2002.