55 Trends for Cyberwar

Posted on March 18th, 2009

55 Trends for Cyberwar

Final Draft

Presented by Dr. Marvin J. Cetron President, Forecasting International

At Future of Information Warfare and Information Operations

Sponsored by JIOPO [Joint Information Operations Program Office], CIA [Central Intelligence Agency], DIA [Defense Intelligence Agency] and NSA [National Security Agency]

U.S. Army War College, Carlisle, PA, March 18, 2009

[Editor's Note: Excerpts about Invincible Defense Technology (IDT) taken from a 171-page report: "55 Trends for Cyberwar" by IDT expert Dr. David Leffler were published in the "Experts Comment" sections. Highlights of Dr. David Leffler's comments:

- Trend #54. Militant Islam Continues To Spread and Gain Power (pages 136-138)
- Trend #55. International Exposure Includes A Growing Risk Of Terrorist Attack (page 141)

Appendix C titled "Utilizing Powerful Peace-Creating Technologies to Combat Cyber Warfare" originally submitted for this report was expanded and featured in the September 2009 *American Heroes Press Newsletter* and it is now available online at *Military Writers*.

This online paper is a copy of the original text. However, in order to facilate ease of reading, it has be reformatted, and hyperlinks to other relevant information have been added.]

Copy of Official US Army Disclaimer regarding this paper:

Director of National Intelligence, or the U.S. Government. This report is cleared for public release; distribution is unlimited."

Table of Contents

Table of Contents…… 2

Introduction…… 3

10 Critical Trends for Cyberwar…….. 8

Expert Observations…….. 23

55 Trends for Cyberwar…….. 51

Population Trends…….. 51

Societal Trends…… 59

Generational & Family Trends…….. 74

Economic Trends…… 80

Work & Labor Force Trends…… 90

Energy Trends…….. 96

Technology Trends…… 101

Environmental Trends…….. 117

Management Trends…… 124

Institutional Trends…… 129

Terrorism Trends…….. 133

Conclusion…… 143

Recommendation…….. 144

Participants' Biographies…… 146

Forecasting International Staff..... 154

Annotated Bibliography..... 156

Appendix A: A Question of When..... 164

Sidebar: The 20 other high-risk Targets 170

Introduction

"Cyber security is the soft underbelly of this country," outgoing National Intelligence Director Mike McConnell declared in a valedictory address to reporters in mid-January 2009. He rated this problem equal in significance to the potential development of atomic weapons by Iran.

With this concern in mind, Forecasting International (FI) undertook a study of factors likely to influence the future development of information warfare. This work was based on a list of 55 trends FI believes will shape the world in the years ahead. In the first stage of research, FI's staff analyzed the probable effects of trends in fields such as economics, demographics, and technology on the course of cyberwar. In the second, we presented this work to 31 leading forecasters, intelligence professionals, and military thinkers and requested their views. This report presents the results.

Director McConnell does not worry so much that hackers or spies will steal classified information from computers owned by government or the military, or by contractors working for them on secret projects. He is afraid they will erase it and thereby deprive the United States of critical data. "It could have a debilitating effect on the country," he said.

Real-world attacks over the Internet also are possible. In March 2007, the Department of Energy's Idaho Lab conducted an experiment to determine whether a power plant could be compromised by hacking alone. The result was a diesel generator smoking and on fire as a result of some malicious data that could easily have been sent to it over the Internet from anywhere in the world. In January 2008, a CIA analyst told American utilities that hackers had infiltrated electric companies in several locations outside the U.S. In at least one case, they had managed to shut off power to multiple cities.

Information attacks have been used in practical conflicts as well. In April and May 2008, Russian hackers believed not to be directly employed by the Moscow government subjected Estonia to a nationwide denial-of-service (DoS) attack that effectively shut down the country's access to the Internet, with substantial economic impact. They began the same sort of attack on Georgia in the run-up to the August 2008 clash between Moscow and T'blisi. Similarly, the military dictatorships of Myanmar and Mauritania both reportedly have hired operators of botnets—networks of illegally commandeered PCs—to smother several opposition websites with DoS attacks.

We conclude that information warfare will be a significant component in most future conflicts. This position is in line with both U.S. military doctrine and white papers published by the Chinese People's Army. One study affirms that as many as 120 governments already are pursuing information warfare programs.

Repeated reports that Chinese computer specialists have hacked into government networks in Germany, the United States, and other countries show that the threat is not limited to relatively unsophisticated lands. A 2007 estimate suggested that hackers sponsored by the Chinese government had downloaded more than 3.5 terabytes of information from NIPRNet, a U.S. government network that handles mostly unclassified material. More disturbingly, *The Joint Operating Environment 2008: Challenges and Implications for the Future Joint Force* ("the JOE") comments that "our adversaries have often taken advantage of computer networks and the power of information technology not only to directly influence the perceptions and will of the United States, its decision-makers, and population, but also to plan and execute savage acts of terrorism."

In a 2008 magazine article, attached as Appendix C, Forecasting International examined possible targets of future terrorist attack. At that time, we were considering vulnerabilities to relatively conventional weapons, such as bombs and toxins. However, many of the targets we identified lend themselves to cyber assaults as well. Consider these examples:

Detonate EMP Bombs in the Internet-Critical Region of Northern Virginia

Probability: Medium

Impact: High

EMP means "electromagnetic pulse," a blast of radio energy so strong it fries electronic equipment. (Set off an atomic bomb at an altitude of 30,000 feet, and there won't be a computer working for miles around.) The terrorists who strike Northern Virginia on 9/11 in 2010 do not need a nuclear weapon to shut down the region's computers. Instead, they use homemade EMP generator-bombs that any good engineering student can build with $400 and information found on the Internet. They detonate nine of the bombs within a triangle stretching from McLean west to Dulles International Airport and south to Chantilly. The EMP blasts take down communications and navigation equipment at Dulles, some of the less critical computers at CIA headquarters in Langley, and data centers that carry some 40 percent of the world's Internet traffic. With police unable to use radios, computers, and cellphones, the terrorists escape. It is eight months before they are identified. Only one of the six-member team will be captured in the next two years. A similar bomb, detonated near Wall Street, acts as a "weapon of mass disruption," sowing chaos and fear.

Casualties: None directly. In Northern Virginia-area hospitals, 17 patients die in part because their computerized monitors no longer operate properly. Another 14 may have

died when their pacemakers delivered massive shocks to the heart and then ceased working.

Consequences: Dulles-bound aircraft are diverted for three days until replacement gear can be brought in. Some 40 percent of the world's Internet traffic flowed through this part of Northern Virginia. Losing that capacity slows the Internet to a crawl, which further complicates emergency response.

Most of the 175,000 people employed in this IT-intensive region will be out of work for at least a year. Repairing the electronic infrastructure will cost an estimated $40 billion. Businesses across the United States lose an additional $2 billion per month owing to the loss of efficient Internet service. The Dow plummets 1,000 points and trading is suspended for three days.

This attack is, of course, a cyber assault even as originally imagined. The same weapon could be used to destroy computer systems in Manhattan's financial district, at financial wire-system centers, or in the government offices of Washington, D.C. According to the best estimates we have been able to find, a good engineer could produce an EMP bomb from widely available parts for $5,000.

Attack on U.S. Oil Refineries

Probability: High

Impact: High

Four terrorists driving minivans approach the gates of four oil refineries: the Royal Dutch Shell installation at Port Arthur, Texas; the Valero Energy refinery at Corpus Christi, Texas; the Chalmette refinery east of New Orleans; and the Chevron refinery at Pascagoula, Miss. They crash through the gates and aim for the key catalytic units used to refine petroleum. The crashes set off more than 500 pounds of dynamite in the back of each van. Eleven workers die in the initial attacks and six more perish in the infernos that send plumes of dark smoke miles into the sky. Even before the flames can be extinguished, the price of oil skyrockets to more than $200 a barrel. The president declares a state of emergency and dispatches National Guard units to protect key infrastructure.

Casualties: Seventeen dead, 34 wounded (several critically burned).

Consequences: In a single day, America loses 15 percent of its crude-oil processing capability for more than a year. The Federal Reserve slashes the prime rate by a full point in a desperate attempt to avert a recession, as gas jumps to $4 a gallon. Critics bemoan the fact that, for decades, the United States neglected development of its "dirty" oil-processing infrastructure—and now it's too late. Total economic cost: $1.2 trillion.

Like many other facilities, oil refineries are almost completely automated. Manipulating their computers to push operating temperatures and pressures out of tolerance could disrupt nation's petroleum supplies as effectively as bombs, with little risk to the attackers. With sufficient preparation, many more than four refineries could be brought down at once. Similar attacks might release toxins from chemical plants or destroy manufacturing facilities.

Bring Down Four High-Tension Wires Across the West

Probability: High

Impact: High

The North American power grid has a dark secret: Of the 10,000 power substations, a loss of only 4 percent will disconnect almost two-thirds of the entire grid. But with proper planning and timing, only 2 percent need be disrupted—downing just a few power lines can have widespread consequences.

Some attacks are as easy as starting forest or grass fires under transmission lines, to ionize the air and cause the lines to fail. Others require suicide car bombs. In 12 hours, by downing just four lines, more than 60 percent of North America is without power. Power is lost from Knoxville, Tenn., to Nevada, and north to the Canadian border.

Casualties: Other than the suicide bombers, there are no direct casualties. But patients in hospitals, nursing homes, and even on respirators and other life-saving devices in private homes begin to expire. The indirect death toll starts to climb rapidly. Based on prior blackouts, 100 to 300 deaths are likely. Stop lights don't work, gas stations can't pump fuel, and civil disturbances occur as crowds waiting in lines to receive ice grow restless. The president considers requesting help from the National Guard to maintain order.

Consequences: Nearly 200 million people are affected, and infrastructure damage could take several months to repair. Even the most optimistic projections show the economic impact could easily top $100 billion.

Again, the power grid is governed by computers that could be manipulated to bring down the system. Oil and gas pipelines, subway systems, and rail lines appear to be equally vulnerable to cyber attack.

Many factors guarantee that the role of information warfare in military planning and operations will expand greatly in the next two to three decades. These include the spread of new information technologies such as Internet telephony, wireless broadband, and radio-frequency identification (RFID); the cost and negative publicity of real-world warfare; and the possibility that many information operations can be carried out in secret, allowing successful hackers to stage repeated intrusions into adversaries' computer networks.

Above all, there is the dramatic growth of technology (our Trend 37.) According to the JOE, “If the pace of technical advances holds true, greater technological change will occur over the next twenty years than occurred in the whole of the twentieth century. In many ways the world of 2030 will be nearly as strange as the world of 2000 would have been to an observer from 1900. The advances in communication and information technologies will significantly advance the capabilities of the Joint Force. Nevertheless, those same advances will be available to America’s opponents and they will use those advances to attack, degrade, and disrupt communications and the flow of information.”

Many of the trends tracked by Forecasting International also will help to shape the future of information warfare. What follows is an analysis of the intersection between FI’s trends and infowar.

Many such opportunities emerge from the trends below, and we would be very interested in any that come to mind. However, our primary focus is not on specific attacks but on the course of information warfare itself. How will these trends make cyber attacks more or less likely? How will they change the nature of the attacks themselves? How will they make it more or less possible to defend the United States against them effectively? What will we face in the years ahead?

These are critical questions for the future of warfighting. The 55 trends examined below will shape the answers. To learn how they will play out, Forecasting International consulted with 28 leading forecasters, intelligence specialists, and military thinkers. Their insights, and our own, form the body of this report.

10 Critical Trends for Cyberwar

We at Forecasting International rate these the ten most significant trends that will shape the future of information warfare. This ranking is based largely on the responses of our expert panelists, but also on our own judgement, developed over 50 years of trend analysis and extrapolation in military and national-security contexts. In nearly all cases, these two inputs agreed.

More detailed examinations of these trends appear later in this report, on the pages noted.

1. Technology increasingly dominates both the economy and society. (Page 85)

New technologies are surpassing the previous state of the art in all fields. Laptop computers and Internet-equipped cell phones provide 24/7 access to e-mail and Web sites. … New materials are bringing stronger, lighter structures that can monitor their own wear. By 2015, artificial intelligence (AI), data mining, and virtual reality will help most organizations to assimilate data and solve problems beyond the range of today’s computers. The promise of nanotechnology is just beginning to emerge…. Ultimately, speculations that we are approaching the “singularity’s event horizon,” the time when

our artifacts become so intelligent that they can begin to design themselves and we cannot understand how they work, may prove correct. At that point, humanity will be largely a passenger in its own evolution as a technological species.

Implications for Information Warfare and Operations: This trend is the ultimate foundation for cyber-war. Complex, often delicate technologies make the world a richer, more efficient place. However, they also make it relatively fragile, as it becomes difficult to keep industries and support systems functioning when something disrupts computer controls and monitors, and the opportunities for disruption proliferate rapidly….

Expert Comments:

Coates –There seems to be a passion moving on to reality to robotize warfare. If it follows the airplane model, any useful number of them could break the bank. As information devices, how will they be fueled in the field? What happens when we retreat and leave them behind, or move out of country? The ubiquity of bright IT clever people has to be integrated into their use.

There is no discussion here of the use of IT by organized crime. I am frequently asked in my public lectures, what students should be studying, through college. One member of the audience said, “What about the Mafia?” One answer is obvious. “IT at MIT,” It is 2015, and the Mafia electronically wipes out the records of a modest sized bank in Texas, or Nebraska or…. And then quietly visits a small group of large financial services organizations with a simple message: “We did it—you could be next. This is what we want, to protect you.”

Forster — Obviously the ability to disrupt the technology infrastructure will have a greater impact on society.

Hoffman — I don’t believe that “dominates” is correct. Technology is being exploited—“very unevenly” by different societies and by different industries to lower costs, increase value, accelerate processes and delivery. Oddly, Bin Laden and his ilk are very effective at exploiting Western technology to promote a non-Western social system.

Pearson — And ever more so in the future. It will become harder to police though, and more dangerous year on year. The benefits will be huge, but so will the risks. There are just too many nutters out there. I think local government and civil service departments make ideal targets, since they are not so well protected as national government, but can cause just as much disruption if attacked.

Sowa — Technology will alter all the current traditional thinking about cyberspace, cyber-warfare, and traditional warfare. Because it will be totally interlinked to the network its ramifications will be costly, and widespread. Battelle Institute, the NSA, the Materials Research Society, NASA, the military branches, and numerous other entities have made significant trend projections in this area. WHAT MUST BE EXPLORED is how, for example, cellular or water-based computing systems, artificial intelligence, and

things like singularity will have specific impacts on cyber programs currently existing, in R&D, in production, or being funded. For example, SEAL Team stealth craft and Navy Destroyers being worked on by Converteam will only remain stealthy as long as the internal wiring and routing system and switches run on fiber—not copper. Yet, current DoD supply vendors do not offer such essential componetry. To handle all aspects of cyberwarfare correctly, these kinds of mindless systemic snafus require adequate futurecasting and analysis. Otherwise, many of our systems will become outdated before they are even production-ready. And, these will greatly add to the total cost of the program—even if short-term budgetary costs are reduced.

Steele — A challenge to information security is an anachronism in Singularity engagement scenario. Cyber systems are cyber realities. Much more holistic in nature—not simply information but cyber cultures. Coordinated cyber attacks at multiple levels will be capable of knocking out macro (national defense systems), meso (local power grids), and micro (starting an automobile) simultaneously.

Thomas — Impact of cyber attack characteristics (anonymity and plausible deniability) on policy and responses: nations have to hold back responses because they can't be sure just who is reconnoitering their systems. Inability to understand impact of culture on methods that nations use the Internet: For example, the Chinese use electrons as carriers of strategies, a concept the US has never followed to the best of my knowledge

2. Advanced communications technologies are changing the way we work and live. (Page 54)

Telecommuting is growing rapidly, thanks largely to e-mail and other high-tech forms of communication. However, Millennials already have abandoned e-mail for most purposes, instead using instant messaging and social-networking Web sites to communicate with their peers. These and other new technologies are building communities nearly as complex and involved as those existing wholly in the real world.

Implications for Information Warfare and Operations: This is one of the two or three critical trends that give information warfare and operations their significance.

As our institutions computerize their operations, they become more vulnerable to unauthorized access. As they redesign their operations to take advantage of the efficiencies computers offer, they also open them to disruption by technologically sophisticated adversaries.

Disruption need not be overt or easily detected. With manufacturing systems increasingly open to direct input from customers, it might be possible to reprogram CNC machine tools to deliver parts that were subtly out of spec—and to rework the specifications themselves so that the discrepancies would never be noticed. If the tampering were carried out with sufficient imagination and care on well-selected targets, the products might conceivably pass inspection, yet fail in the field. This could have significant military implications.

Expert Comments:

Callanan — Advances in information and communication technology have clearly meant that the mobilisation of all sorts of groups pursuing a wide variety of causes is both easier and cheaper. Virtual networking can be reasonably expected to lead to a proliferation of a larger number of smaller "specialised" extremist groups, some of whom may spend as much time vying with each other as much as anything. Nevertheless, this presents the security community with the daunting task of fronting up to a far more diffuse threat than until now.

In terms of cybercrime, one can expect the main focus of the intelligence community to be around a three-pronged approach: detection; interception and intervention to undermine the technology infrastructure of extremist groups; and influencing.

Coates — As everyone recognizes, the Internet is a mess, open to all kinds of uses, misuses, anti-social material, irksome intrusions from ads, identity theft, international swindles, and on and on. … For these reasons, as well as the potential for national security interventions, and general hell raising, it is time to plan, design, and execute over the next five to seven years, a replacement for the Internet.

Forster — New communication technologies will further change the way conflict takes place. First, the ability to utilize communication technologies to achieve information superiority and dominance is essential. Second, denying others access to information will also be critical. Third, the ability to exploit information effectively will reduce the current asymmetrical differences between states and between states and non-state actors. For example, the size of the military will matter less than the ability to effectively use information to determine weaknesses and strike.

Kauffman — Non-nuclear EMP (electromagnetic pulse) bombs may be a serious danger for both military and civilian systems

LaDuke — Intelligence technology of the future will have three main fronts:

1. The traditional approach of communication interception,
2. Threatening intention detection through technology and
3. influence or persuasion to change intention.

Pearson — And also creating more vulnerabilities and more dependence. The "Age of magic," where only a few elite understand how stuff works, could lead to abuse of that power, just as the high priests held high power in old civilizations.

Snyder — In fact, communications has already begun to supplant travel—e.g., tele-commuting, virtual vacations, distance learning, and digital recreation.

Sowa — Impact is felt to be higher than the authors suggest.

Steele — Global cultural interactions will produce unexpected outcomes and potential challenges to global stability. Not only will continued intercultural synthesis increase, but non-nation-state combatants will be joined by cyber system combatants (in singularity engagement). Some will be human controlled, some will be cyber system controlled (machines creating and controlling themselves). Cyber-cyber engagement may rely on a cyber system's ability to "out-evolve" its cyber opponent. Literally, beyond human control.

Thomas — Psychological operations closely connected with social engineering: social engineering leads people to make certain selections on the Internet, and thereby can influence attitudes just as psyop does.

Impact of new media (blogs, ICQ, etc.) on cognitive processes and search for truth: spread of fake messages, altered images, YouTube videos are new methods of spreading news, sometimes to spread disinformation.

van Klaveren — I am presently involved in exploring virtual worlds and their possible applications. It is a certainty that "virtual worlds" will become a very important force in general life and especially in education. If one interacts with participants in Second Life—and have them tell you how much their real life ideas and attitudes are affected and modified by their participation, you can only conclude that virtual worlds will have a major effect on the way our cultures evolve. There are some very worrisome developments—but the potential for "good" is also tremendous.

Vogel — There are two technology-related areas that I believe that will impact—at least in the near- and mid-term—several trends listed in the paper, "55 Trends for Cyberwar:" cloud computing and Web 2.0 applications.

Cloud computing is a shorthand description of service-oriented computing. …

Rather than installing and maintaining the application on each of our PCs or servers, we rely on a third party to host and maintain the application and pay only when we access the application.

… Gartner analysts Daryl Plummer and Thomas Bittman at the Emerging Technologies conference in Las Vegas, made the predication, "By 2012, 80 percent of Fortune 1000 companies will pay for some cloud computing service, and 30 percent of them will pay for cloud computing infrastructure." …

The cybersecurity implications associated with cloud computing, whether a public or private cloud, are significant. As more companies and the government adopt cloud computing, they become more vulnerable to disruption and cyber attacks. This could result in disruption in services and the ability to rapidly access critical software applications.

Web 2.0 applications. With the wide-spread use of Facebook, blogs, and other social networking applications in our personal lives, government organizations are seeking similar capabilities for communicating and interacting with their stakeholders. … Once the government permits interactive, two-way communications over government networks, the chance for cyber attacks dramatically increases.

3. The global economy is growing more integrated. (Page 67)

Critical factors here include the rise of multinational corporations, the relaxation of national distinctions (i.e., within the European Union), the growth of the Internet, and computerized outsourcing of jobs to low-wage countries.

Implications for Information Warfare and Operations: For "integrated," read "networked." The Internet, private networks, virtual private networks, and a host of other technologies are quickly weaving the planet into a single, massively complex "infosphere." These nearly infinite connections cannot be severed without overwhelming damage to companies, and even national economies. Yet, they represent unprecedented vulnerabilities to espionage and covert attack. This is another major trend for information warfare and operations.

Expert Comments:

Forster — Greater economic integration increases interdependence and thus the ripple effect of disruption is far greater. … As a result, anything that disrupts the economy, such as a power outage caused by a hacked power system, will have a broader impact….

Hoffman — Concur that interdependencies and even inadvertent linkages and networks are increasing vulnerability to cascading effects. Many of these networks are one step removed from effective security and expose numerous sites and individuals to unknown risks. Security and resilience systems are not keeping up.

Kapinos — Another thing to think about here: the sheer volume of information racing through the "info sphere" enhances the opportunity for cyber-war operators to embed encrypted information within routine data flows. This could take the form of system-disabling viruses, or secret message traffic concealed within an ocean of regularly-transmitted, legitimate data. … Sophisticated data-monitoring programs designed to detect unusual patterns would be needed to counteract such a scheme.

Pearson — This leads to more complexity of interactions, so it will be harder to spot points of vulnerability. Fraud and cyber terrorism will increase.

Peterson — This I believe is the ultimate Achilles heel—but it's not limited to the economy. Physical networking integrates all global, national, and interpersonal C4I—government, military, commercial and social. How do you kill a hostile, self-replicating,

avatar that takes residence in every device/multiple network buffers and attacks as part of the “call set-up” protocol in node to node contact?

Sowa — THIS IS A CRITICAL FOLLOW-ON TO MY NOTE FOR TREND 18: Corporations in the 21st Century are borderless and are NOT geopolitical. Ninety percent operate with a stated purpose to “maximize profits” for their stakeholders. In such an integrated global economy, shocks to the system, as I said in 18 have system-wide repercussions. Only the extent of the damages varies from shock to shock. Cascading failures are often-cited and emergent phenomenon in any network. They are NOT independent, nor are they coincidental. The key to actively thwarting Cyberwarfare is to recognize corporations and organized religions on the same—or even higher protocol—than geopolitical governments and borderless, non-geopolitical terror and extremist operations.

Cyberwarfare actors in these may or may not be acting with purposeful negative or criminal intentions. They may be acting for purposes to maximize profits for their stakeholders—who may not be of country-of-origin. But, in all cases they do represent unprecedented vulnerabilities to espionage and attack—AND AS SUCH ARE VERY LIKELY TARGETS TO ACT AS A “BASE” OR STAGING GROUND FOR FURTHER ESPIONAGE OR CYBER-ATTACKS.

Because of the interconnectedness, Corporations infiltrated by electronic, or by outsourced hiring practices can cause major mayhem and disaster to the networks of cyberspace. And, if not managed against, because we have integrated many of our infrastructures—including cyberspace, and the electronic means to run our manufacturing and businesses—as well as the interconnectedness of our water supply, military materiel, energy and power transmission, oil and chemicals, biologicals, poverty, food, and even our ecosystems—we are now all impacted by any failures within these systems—and we should remain diligent on the ramifications of much more grave systemic threats and the global cooperation needed to implement a cooperative gridwork control system to avert the worst crises.

The ramifications of this to strategy and tactics in Cyberwarfare should be obvious again. The potential systemic threats here are very highly probable as a threat at this juncture, and none of the mitigating solutions so far even take into account natural phenomena.

4. Research and development play a growing role in the world economy. (Page 71)

Total U.S. outlays on R&D have grown steadily in the past three decades. Similar trends are seen in China, Japan, the European Union, and Russia.

Implications for Information Warfare and Operations: This trend is responsible for the accelerating technological advances seen in recent decades. It is another critical factor in the development of information warfare.

The chief product of R&D is not clever new merchandise or technologies, but information. Even the most sensitive output from research results are routinely stored in computers, shipped through company intranets, and usually transmitted over the Internet. This accessibility makes it a prime target for espionage, whether industrial or military. This problem has been growing nearly as quickly as the mass of information available to prying. It will be a still greater concern for security specialists in the years ahead.

Expert Comments:

Anonymous — Spending on R&D for a growing company has to be about 10 to 15 percent of what is plowed back into the company, or the company dies. This has been true for at least the past 30 years. So this trend is not an increase unless you are talking about an R&D budget in excess of 15 percent, which I would find difficult to support, either as a company officer or as a future trend.

Callanan — You might also wish to consider the emphasis that is placed within many R&D programmes on the dissemination of research results. While this is of course entirely sensible for the vast majority of research, the emphasis on getting as much information “out there” may pose additional security dilemmas in terms of cybercrime.

Pearson — Of course, the downside is that R&D also occurs in weapons tech, so there is always a background arms race. High capability technologies will present enormous threats to mankind in the second half of this century. I estimate average date of expected extinction as 2085. By accident or design.

Peterson — This isn’t true in real dollar terms. Incremental product engineering is now labeled R&D. The real innovation centers are obsolescent and substantive breakthroughs are fewer and farther between, and diffusion and assimilation rates are slower. Spin of packaged data not-with-standing; what is the market place telling us (university incubators, PARC, Bell Labs, etc.)?

Sowa — Research and Development—and especially the development of new technologies in every field—will continue to be the “great hope” that the world embraces to keep the economies and governments successfully operating. The value of R&D throughout history has been evident in all means of social, economic, political, and military success. Over the next 20-year cycle, R&D, and innovation from R&D, will accelerate exponentially in every country of the G20—and beyond into the developing world.

In a more narrow range of cyberspace, new technologies will hold the keys to cyberwarfare, cyber-security, and cyber-attacks. This is a target-rich environment for espionage and attack. The actors to be defended against must include the traditional geopolitical organizations, but also the borderless, and non-geopolitical players mentioned prior, and the single lone- or small group actors.

5. The pace of technological change accelerates with each new generation of discoveries and applications. (Page 94)

In fast-moving engineering disciplines, half of the cutting-edge knowledge learned by college students in their freshman year is obsolete by the time they graduate. The design and marketing cycle—idea, invention, innovation, imitation—is shrinking steadily. As late as the 1940s, the product cycle stretched to 30 or 40 years. Today, it seldom lasts 30 or 40 weeks…. The reason is simple: Some 80 percent of the scientists, engineers, technicians, and physicians who ever lived are alive today—and exchanging ideas real time on the Internet.

Implications for Information Warfare and Operations: As new technologies arrive, industry will be forced to hire more technology specialists and to train other employees to cope with new demands. Some support functions may be moved offshore, where technically knowledgeable adversaries might have greater access to them, opening the way to disruption. …

Expert Comments:

Coates — It is important in the discussion not to neglect the large amount of information technology now obsolescent or obsolete, but in place. We did a small and unclassified study of that subject for the NSA a few years ago.

Forster — Proliferation of technology facilitates the coalescence of unrelated but networked organizations (criminal and terrorist) in the execution of an operation.

Hoffman — Yes the potential for greater convergence of various technologies will accelerate the development and introduction of new systems and techniques. This will require constant adaptation by systems managers and constant learning at the individual level. Whatever you were taught in undergraduate school is certainly going to be obsolescent before you take a graduate degree. Does our educational system support this? Do government personnel systems recognize this?

LaDuke — … Knowledge creation is a repeatable process that is performed by humans and could be performed by machines exclusively or in systems built to interact with humans (“Man-in the-loop” systems). Artificial knowledge creation (AKC) will usher in singularity, not artificial intelligence (AI) or artificial general intelligence (AGI) or technology advancing itself. Artificial intelligence (AI) has already been achieved by any computer because intelligence is appropriately defined as knowledge stored that can be retrieved (by human or computer).

The first arriver to this technology will drive the entire paradigm shift.

Pearson — The singularity is a real risk, when new weapons or analysis of existing systems to find security holes becomes too rapid.

Sowa — This trend has a “high” impact and probability.

Steele –A Scenario Builder -Toward a model of cyber combatants, 2035. While there are many variables that influence cyber war, this model reflects the intersection of the level of the technology involved and the nature of the combatants. It is offered for reflection and further development if relevant. It is a typology that sets the stage for a multiple outcomes.

Examples:

The first two elements (Human-human and Technology/Cyber Enhanced) are familiar as they reflect human evolution on the planet to this point. The elements suggest everything from hand-to-hand combat to smart and intelligent weapons used by humans on humans. This is the current state as increasingly smart weapons engage humans (simple example, drones) and cyber system on cyber system launched by humans.

Singularity engagement suggests cyber systems creating AI and technological weapons and using them independent of or engaged with humans.

6. The United States is ceding its scientific and technical leadership to other countries. (Page 89)

“The scientific and technical building blocks of our economic leadership are eroding at a time when many other nations are gathering strength,” the National Academy of

Sciences warns. “Although many people assume that the United States will always be a world leader in science and technology, this may not continue to be the case inasmuch as great minds and ideas exist throughout the world….”

Although R&D spending is growing in raw-dollar terms, when measured as a percentage of the total federal budget or as a fraction of the U.S. GDP, research funding has been shrinking for some 15 years. … Only half of American patents are granted to Americans, a number that has been declining for decades.

More than half of American scientists and engineers are nearing retirement. At the rate American students are entering these fields, the retirees cannot be replaced except by recruiting foreign scientists….

Implications for Information Warfare and Operations: To whatever extent the United States loses its leadership in science and technology, it falls behind other countries in the intellectual and personnel base required for information warfare and operations. If this trend is not reversed, the U.S. could find itself at a significant disadvantage in this strategically and tactically important area….

Expert Comments:

Anonymous — I find that the number of person’s entering a field is not the important metric. The quality of those people is the critical measure.

Coates — I think that half of your first sentence is unsustainable, that our scientific and technological building blocks are eroding. There is confusion between other countries doing better, implying that we are doing worse. It can only be good for humankind if we have numerous centers of excellence rather than follow some football game model, that you are on top or you are nothing. Again you repeat the point, or more properly the allegation, that our technological capabilities are deteriorating. I must see an article every two weeks claiming that—and offering no support.

Hoffman — A bit alarmist in tone, we had an artificial lead in some respects due to the second World War and even the Cold War. Yes, this advantage is slipping over time, but as Zakaria and Berkowitz have written in their books we retain a lot of systemic advantages. The world is returning to a normal distribution of power, and we retain advantages in size, allocation of capital, rewards and incentives and education. Overall, our position is diminished and we need to be conscious of how we can best preserve a competitive advantage.

LaDuke — The strength of the U.S. is in knowledge creation under the auspices of innovation and invention that has been applied in all kinds of technologies. Ceding existing technology as technology converges and rises exponentially is not as significant as not creating the knowledge that is empowering future advances in technology. Any looking backward at threats is at the least distracting and at the most counterproductive.

Pearson — The increased power of smart individuals is more of a problem, espcially in NBIC areas. Unabomber style activity from inconspicuous people within a community is more of a danger than hostile states or terrorist groups.

Sowa — The impact and fallout of losing scientific, technical, and engineering leadership is a high-risk trend. The US will lose its standing in all areas—militarily, economically, and socially. This threat is far-reaching. Russia and Bulgaria are mentioned as high threats—but the list should actually include much of Eastern Europe, and former satellites of the USSR, as well as our "neighbors" in North, Central, and South America, Micronesia, Indonesia, and the Caribbean.

Steele — Not only is the U.S. ceding the "left brain" sciences, but the continuation of a linear, industrial model for education has the U.S. ceding a growing need for "right brain"—creative and synergistic thinking. Humans (and transhumans, androids on one hand and genetically altered humans on the other) living in the "Singularity Engagement" era will need thinking with left and right brains and synthesize direct information upload to the human brain.

Failure to adopt 21st Century thinking. Systemic failure to rapidly create processes for combating and thinking about nonparadigmic states of being produces vulnerability. Searching for questions with multiple answers (vs. paradigmic searching for "the right answer…") becomes a way to engage cyber war in the current and future century. Intense training in this "way of thought" that is beyond creative problem solving but rather creative reality creation enhances societal capability and human capacity.

7. Technology is creating a knowledge-dependent global society. (Page 99)

More and more businesses, and entire industries, are based on the production and exchange of information and ideas rather than exclusively on manufactured goods or other tangible products. At the same time, manufacturers and sellers of physical products are able to capture and analyze much more information about buyers' needs and preferences, making the selling process more efficient and effective. …

Implications for Information Warfare and Operations: Increasing dependence on technology effectively translates to growing fragility. Disrupt essential information or communications systems, and a company, government agency, or military unit could be dead in the water, or at least cut off from oversight and coordination with its partners. Telecommuting systems, for example, offer several obvious opportunities to disrupt the operations of the company or agency that depends on them.

Expert Comments:

Ayers — The "bunker-buster" ammunition that could be brought to bear within the context of cyberwar has not yet been deployed (or at least apparently not yet in a manner that has worked well). How knowledge-dependent populations react—or how

“new media” societies are capable of reacting—when such weapons are deployed, may ultimately determine their fate.

The chaos that could be caused either under a limited (homemade) EMP scenario or as a result of one or more high-altitude nuclear blasts would be devastating to a Western population in many ways. The losses incurred would make the current economic downturn seem like a mere irritant. Obtaining long-term assistance—whether in the form of backup electronics and parts, or merely food, water, and shelter—would be difficult even if only for a relatively small region within the continental United States. …

Coates — Many regions of the world, either neutral or favorable to us, may be victimized by IW, cyberwar, and we may therefore need to look at how to assist them, at this stage generically; later, specifically.

The problem is open as to how we might assist our long term allies, e.g., the U.K., should it undergo an IW attack.

Kapinos — It is important to consider that there is likely to be a strong relationship between cyber-crime and cyber warfare. Coming from the perspective of the law enforcement community, and working as a strategic planner within that community, I continually stress that much of the crime that we will be faced with in the future will be electronic in nature (cyber crime). In his famous 1970 novel *The Godfather*, Mario Puzo said that “a good lawyer with a briefcase can steal more than a hundred men with guns”. Today, I would paraphrase that to say that an inventive hacker with a laptop can steal more than a hundred lawyers with briefcases. Certainly, one of the things that could be stolen, altered or destroyed is information of all sorts.

I would also suggest that cyber-criminals (even seemingly innocuous ones) pose a potentially much greater threat than many believe. …

With this in mind, I believe that it is crucial for the law enforcement and intelligence communities to work in concert to identify, and address the sources of cyber threats. …

LaDuke — …The current social order of knowledge working based on expertise, political factions, and physical boundaries is on a collision course with the fundamental nature of knowledge. As we rise toward ubiquitous computing, this conflict will become more and more apparent.

Rowlatt — …Counter measures to cyber threats developed by us will impede our ability to work effectively let alone efficiently. Firewalls, authentication, and encryption programs have the potential to slow the flow of information. An enemy would love to slow down some decision cycles. This approach would allow them to achieve the aim simply by presenting a threat be it credible or virtual.

We become distrustful of information contained or processed within cyber networks.

Sowa — Our existing high-priced cyber-system remains extremely fragile and vulnerable to grave systemic attacks. Our main defenses are based at the perimeter. These defenses will continue to minimize access, and thereby thwart common attacks well into the future. Newly found TCP-IP and DNS threats; switch and router threats; as well as threats caused by poorly-determined and thought-out approaches by vendors (i.e., client-based server control, etc.) will continue to propagate vulnerabilities and security risks. Smart phones, sub-netbooks, PDA's, wearables, RFID technology, and nano-technologies that can alter clothing fabric into computer storage units—will continue to alter the technical threats that have to be foreseen and planned for.

Steele — A single dominant nation-state is a declining reality. The rise of the "cyber state"–potentially cyber created and maintained existing in cyberspace (without geopolitical boundaries–without a label "China, Asia, North America, etc.") will join the collection of geopolitical nations.

Thomas — Departure from a global village to a segmented society: There are now thousands of specific sites on the Internet for ideologies of all types which, at the moment, have done as much to divide nations as to integrate them.

8. Militant Islam continues to spread and gain power. (Page 118)

It has been clear for years that the Muslim lands face severe problems with religious extremists dedicated to advancing their political, social, and doctrinal views by any means necessary. … The overthrow of Saddam Hussein and the American occupation of Iraq has inspired a new generation of jihadis, who have been trained and battle-hardened in the growing insurgency….

Implications for Information Warfare and Operations: This is one more category of attack that Muslim radicals could mount against their chosen enemies in the West.

One likely source of such an attack would be India, a land with a substantial Muslim minority, about 150 million people, and strong computer and communications industries.

Expert Comments:

Ayers — It has long been noted that radical Islamists have been using the Internet to preach, recruit, glorify suicide-bombers, and perform training on a global basis. …The "e-possibilities" for Islamic militants are obviously limited only to the imagination, just as they are for more harmonious or legitimate activities. … the cyberworld offers a wealth of opportunity to engage in the spread of Islam, followed by or in conjunction with a cyberwar that would be seen as "just" in the Islamic tradition.

Coates — The information technology aspects of terrorism, small wars, civil wars, and rebellious activity must be thought through afresh, with the primary goal to be winning over people and making them secure in their own terms.

We must develop a policy which throws disruptive events into a realistic framework for effective public policy. …contingency plans of an unfamiliar sort should play a larger and fresh role in military and public policy planning.

Forster — Technology proliferation & communication technologies are facilitating the recruitment, indoctrination, funding, training, and operationalization of terror groups worldwide. As has been known for some time, Al Qaeda is no longer a centrally controlled organization but a networked organization. Information technologies have improved its internal security while permitting cells to coalesce only at the time of attack. … However, on the positive side, terrorist groups also are more dependent on technology; therefore, successful attacks on their technology infrastructure do more to disrupt planning and execution.

Hoffman — I don't concur with expanding or growing influence of Islamic extremists. These are near term conditions, and an equally valid historical argument for religious extremists and terrorist groups to burn out. See the literature on Audrey Cronin regarding the shelf life of terrorist [movements.]

Sowa — Cyber-attacks by perpetrators will persist. Some portion of the perps will be terrorists that don't care if the mission is suicidal. Some of the more radical examples of possible attacks have already been discussed.

Thomas — Internet ability to cyber mobilize: Internet can train, finance, recruit, etc.

9. International exposure includes a growing risk of terrorist attack. (Page 123)

Terrorism has continued to grow around the world as the wars in Iraq and Afghanistan proceed, even as the rate of violence in Iraq itself has declined. … Nothing will prevent small, local political organizations and special-interest groups from using terror to promote their causes. … On balance, the amount of terrorist activity in the world will continue to rise, not decline, in the next 10 years. … In fact, terrorist attacks had risen sharply since the invasion of Iraq, both in number and in severity.

Implications for Information Warfare and Operations: Until the terrorist problem is brought under control—probably not for at least a generation—we will face a growing threat that Muslim extremists will master computer and Internet technologies and use their skills to disrupt essential communications and data. The impact will be seen in American corporations, research laboratories, universities, utilities companies, and manufacturing. Cyber operations will be at best second choices for many terrorists, who prefer newsworthy gore of attacks with bombs and firearms. However, their potential for maximum economic impact with minimum risk eventually will make them irresistible to forward-looking extremists.

Expert Comments:

Ayers — As evidenced from previous attacks, Osama Bin Laden probably sees the vulnerabilities of his enemies through the eyes of experience associated with civil engineering (whether that experience was obtained from the family business, from later education, or both). …

Bin Laden's cyber equivalent will undoubtedly view vulnerabilities—and the potential for destruction–quite differently. The cyber attacker sees the enemy as an object to prod and probe with little (if any) fear of capture and containment. … The effects achieved may be well worth any extra effort extended—especially if the entire operation can be performed from a safe location thousands of miles from the target. A relatively small effort may produce wide-scale damage to enemy infrastructure and possibly even result in casualties. …

The Internet has facilitated the cooperation of "groups with grudges" (large and small), and in-so-doing, enhanced the ability for each group to capitalize on their own strengths—ultimately becoming part of (through a loose affiliation) a bigger, more aggressively confrontational, and more capable entity. …

Cyber terrorists can use methods to hide their activities that are extremely difficult for law-laden Western counterterrorism experts to locate. … If you add the vast array of social networking sites (e.g. YouTube, Facebook, and a multitude of blogs), you have a very big problem.

Regardless, cyberwar attack modes have already been tested. … There seems to be little doubt that the worst is yet to come.

Forster — Cyber capabilities mean an increase in attacks both from terrorist organizations and individuals who have access to a computer and the "know how" to hack into systems. The increases in vulnerabilities mean additional resources need to be spent on protection and mitigation.

Hoffman — Concur with Frank Sowa on the persistence and adaptation of attacks. Our increasing urbanization and concentration of resources increases our vulnerability, leading to attempts to conduct "systems disruption" attacks per the Open Source Warfare construct of John Robb.

Rowlatt — National security needs to address the freedom big business has in moving its IT services off shore. If a business is a major contributor to a nation's GDP, then what right does it have to expose its Cyber Underbelly, to a foreign power, which in turn, exposes the nation to unnecessary cyber risks? Look at how terrorists targeted Mumbai which is the cyber centre for India, which serviced many international organizations IT needs.

Sowa — Cyber-attacks by perpetrators will persist. Some portion of the perps will be terrorists. The attacks should move over the next 20 years from solely physical attacks to combination cyber- and physical-attacks to a focus of cyber-attacks as stated to a

complex attack designed to carry out a specific mission toward a greater end (similar to U.S. shock and awe strategic planning when we attacked Saddam Hussein—on a dramatic, but much smaller scale—i.e. oil refineries, nuclear plants, chemical plants, harbors, subways, entertainment facilities, hospitality and restaurant facilities, financial facilities; or Mumbai-style attacks).

10. The world's population will grow to 9.2 billion by 2050. (Page 36)

Early versions of this report predicted that the world's population would double by 2050, and population growth has proceeded almost exactly on schedule. Unfortunately, the greatest fertility is found in those countries least able to support their existing people—the Palestinian Territories, Yemen, Angola, the Democratic Republic of Congo, and Uganda. In contrast, populations in most developed countries are stable or declining. The United States is a prominent exception.

Implications for Information Warfare and Operations: The world population's growth is less significant than where those people are concentrated. India already has the largest supply of English-speaking scientists, engineers, physicians, and technicians in the world. China soon could have the largest population of technically trained workers on the planet. A small fraction—but probably a very large raw number—will have the skills needed for information warfare and operations. Beijing already has stated its goal of being able to fight and win "wars under conditions of informatization." Under these circumstances, that country's population represents a mil-tech asset that the United States cannot hope to match, save by superior education and training.

Expert Comments:

Hoffman — Here again a bit of detail is needed to uncover potential implications. More than 80 percent of the population growth will occur in Asia and Africa. The educational **systems** in the latter will not support the advancement of knowledge workers to any degree, and could be swamped by poor governance, lack of services, and chronic disorder. Many places in Asia will experience some of the same downsides of large population growth without adequate governance, services, and education.

Pearson — Increase in population comes with increase in number of malicious people too, as well as more benign people to tackle problems.

Sowa — HIGH PROBABILITY: Cyberwarfare in the 21st Century will target infrastructure to gain strategic and tactical advantage, trade and intellectual secrets, and enhance passive monitoring to gain power and money. The lack of technically-sophisticated westerners poses one of the largest threats here through 2030 as the U.S. ages rapidly.

Steele — Disproportionate segments of world's population growth in the developing world will produce a widening gap between developed and developing worlds. This produces environments of anomie and alienation as a breeding ground for terrorist

ideology. Yet, a growing proportion of the world's population (including the developing world) is gaining primary and secondary school equivalent education. The diffusion of cyber systems in the developing world increases opportunity for global cyber war.

Expert Observations

Anonymous, Senior Intelligence Officer, Joint Staff Directorate for Intelligence, J2

While I'm certainly not an expert on cyber war (I'm kind of a Luddite when it comes to technology, let alone some of the newest technologies you describe), I am a bit troubled by the overall tone of the analysis and response from the "expert" panelists. As futurists, they seem to fall prey to easy, dire predictions followed by linear projections all ending in some form of immanent gloom and doom. I've found most terrorists and evil-doers to be just a touch crazy, no? They seem to be capable of almost accomplishing their goal, but never get much further than creating some initial "shock" which invariably gets built up into "awe" by the 24 hour news cycle.

For instance: A conventional EMP attack, as you describe, is little different from the old "bolt from the blue" Soviet EMP attack on North America. When confronted by what we feared was their "plan" after the Cold War, Soviet professionals simply laughed. They knew that even if they could cause disruption with a surprise EMP attack, it would still take months to mobilize. They could not capitalize on tactical surprise, and that merely served to awaken us, which ensured their defeat—as they modeled it. Some similarities can be extended to the various terror attacks you describe. Shock without preparation is irritating vice devastating, I think.

Also, I think the economic downturn has already had a significant affect on technology driven as well as conventional globalization. I'm just spitballing here, but play long with my "what if" for a moment. "What if" the high water mark of globalization and the high water mark of elected, pluralistic government both have been reached for now? The first signs of what may be four major indications are emerging in Latin American and Russia.

1. Decline in world trade. A new article in the *Economist* details the drop in trade among global markets. Specialization in a global market place is being replaced by generalization in local markets.
2. The rise in self-sufficiency movements and various forms of isolationism. The decline in profits from specialization to compete in global market places will encourage a growth in the domestic production of goods to meet the demand for items that can no longer be obtained from the global market place. Prices for locally produced goods will increase, but localization of production will produce more and different jobs than globalization did. Regional markets might replace the integrated global market.
3. More nationalizations. The Bolivarian countries, led by Venezuela, have been ahead of the times in spearheading a revival of nationalization, but for socialist reasons. Ecuador, Argentina, Bolivia as well as Venezuela have been in the lead in expropriating the assets of multi-national corporations and in rewriting the

terms of business. Other nations will follow as the economic consequences bite deeper. No government can withstand the allegation that it has allowed foreign companies to prosper at the expense of the well-being of its own populace. Expropriation of multi-nationals is good politics and maybe good business, in the short term, irrespective of neo-socialism.

4. The rise of authoritarian governments promising reform and better times. Strong willed leaders who promise reform, an end to corruption, and a free lunch might sweep elections and sweep out pluralistic democracy. The leading edge of this trend is Russia, Venezuela, and Bolivia. Consultative, elected, deliberative government is too slow, too expensive, and too stodgy to respond effectively to emergency needs in poor countries. Demagoguery will have a new day.

All this put together changes the landscape. I think some of the trends you describe as well as the rather linear projections were extent in the political, economic, technological, and social climate of six to eight months ago. The global economic crisis is a tectonic shift whose effects are not fully developed. Yes, technology marches on. Even I am considering investing in a MacBook Pro to replace my ten year old Dell… But, the affect of technology on a changing political, social, and <potentially> more regional and isolationist polities has yet to be adequately assessed. I guess my bottom line—and concern with the uniformity among your experts—is that most of the assessments and projections seem to be artifacts of the last war (9/11). The next war is now.

Anonymous source at the UK Ministry of Defence

These expert contributions all help to emphasise both how important this area is and how far we have to go if we are mitigate our own vulnerabilities. The following are some personal observations, which we hope will be of benefit.

a. **Leadership and Organisation**

Establishment of pan-government, integrated cyber programmes and capability. There is a need to identify a single organisation to lead, manage and execute national cyber capabilities. Capabilities will need to be established across government in tandem with developing a co-ordinated strategic cyberspace programme.

Ownership of cyberspace capabilities. A specific concern for militaries is that there is as yet, in most Western militaries, no acknowledged owner of cyberspace. This in turn means that no-one organisation is specifically focusing on how to protect key capabilities against cyber-attack but also how to develop a coherent cyber warfare capability.

Cyberspace operations will require a new class of cyber cadre. Effective cyberspace operations will necessitate the recruitment of cyber warriors, either as operators or analysts, and the nature of the cyber threat will mean that significant numbers of these specialists will be required – this will be challenging. Particular focus will need to be given to developing career paths, and the right organisational structure, along with the necessary education and training. In developing the cyber cadre, there will also be a

need to understand the wider issues relating to socio-technical systems and non-equipment capabilities, such as the human factors and cultural issues faced with information management and exploitation. More specifically, research will be needed to assess areas of human behaviour and performance (including cognition and perception); selection, training, and recruitment should be targeted if we are to grow and develop the requisite expertise.

b. **Doctrine and Taxonomy**.

There is currently a lack of agreed definitions for Cyberspace and related activities, recognising the need to refine doctrine and organisational structures to match potential (sovereign) national requirements. Development and review of doctrine should be proceeded by conceptual approaches. Conceptual approaches need to be developed and informed by; relevant experiences; lessons learned; historical and scientific evidence; and the development of analytical models/experimentation, including scenarios/vignettes, to understand the impact of cyber operations.

c. **Legal Issues**.

Assessment of the legal implications of cyber activities, and establishing a legal framework for conducting cyber operations. The need to assess the measures of effectiveness of cyberspace operations and provide 'appropriate' response, whether concerning national security or domestic/commercial law enforcement is a critical area that is not really covered in the paper. Whilst our adversaries will not necessarily be constrained by societal norms or rules – we do not have that freedom and must therefore ensure that we operate within the framework of established and defined rules. The decision loop for Cyberspace activities is underdeveloped and uncompressed, unlike the sensor-to-shooter cycle and this loop will require to be closely controlled.

There is a need to also focus on the attribution of cyber attacks; whether at state or non-state actor levels, and the challenges in understanding discrimination, proportionality and national necessity in cyberspace – especially because of the reliance on 'dual use' systems. Cyberspace operations need to have an 'equivalence' to kinetic action, and we must be able to understand the 'intent' of attacks irrespective of the physical or cognitive effect desired, whilst assessing the implications of Cyberspace operations. This activity should engage both civilian and government legal advisors, and the international community, towards establishing a robust legal framework.

John C. Coale—Technical Director, Department of Defense

Top Trends Impacting Cyberwar, February 2, 2009

Caveat: After tracking technologies as an electrical engineer and intelligence analyst for over 30 years, these are my personal predictions of trends impacting cyberwarfare. The opinions expressed here are my own and not necessarily those of the DoD.

- By 2009, Cyberwar becomes a normal occurrence. With the cyberwars of 2007 (Estonia), 2008 (Georgia), and 2009 (Kyrgyzstan), Russia and China continue to demonstrate their capabilities to disrupt e-commerce and steal intellectual property at will without repercussions. Their efforts continue with Russia attacking Ukraine over political disputes and China attacking U.S. national interests.
- By 2010, every 5 to 10 years will constitute a computer generation of people. Each generation will double their capabilities to use and abuse technological systems. Cyberwars will be for the young and restless, who will be 2 to 4 times smarter technologically than their supervisors and parents.
- By 2012, the convergence of online gaming, social networks, and virtual worlds which now drives the entertainment and communication businesses will drive all interactions. This will change how we think of privacy, security, and reality in 3D environments. Since Asia is driving this market (and the Middle East is increasing its participation), the U.S. may be behind in understanding and utilizing these technologies in a cyberwar.
- By 2015, our personal communications e-devices will be speech-enabled, small, mobile, wireless, and wearable. The “Star Trek” lapel pin will be the wave of the future with an “iPhone-like” device for graphics and textural information. Soon thereafter, these devices will be hacked, impacting cyberwar strategies.
- By 2017, English will not be the most commonly used language of the Internet. With an increasing Internet population, especially by Asian countries, Internet standards, protocols, and language will change, impacting the way cyberwars are conducted and the U.S. primacy in these wars.
- By 2020, with the advent of IPv6 and RFIDs, everyone and everything will have an IP address. All devices and IP users will “synch” with every other device or user, meaning that privacy and security will be a thing of the past. The ability to keep a secret will depend on the restricted societal and cultural norms of non-democratic countries. The U.S. will be more at risk in a cyberwar or conducting one.
- By 2022, the U.S. will become less and less of a leader in these technologies, making us more dependent on others for privacy and security. Cyberwars will be to the advantage of those in control of the standards, protocols, and democratic (rule of law) restrictions.
- By 2025, the (cloud, nano, optical, and/or DNA) computing power and storage capabilities will increase to the point of storing all human knowledge. Anyone will have access to any knowledge. Cyberwars against nations can be waged by an individual as well as nations against single individuals.
- By 2028, this increased power and capability will make it near impossible to tell the difference between human and AI. Cyberwars may be waged in the mind of an individual, a network, or a system without being “heard” until the unintended or secondary consequences are felt.
- By 2030, all knowledge and e-devices will become so interdependent that no one will be able to conduct cyberwar without hurting themselves.
- By 2035, all wars including cyberwars will be conducted for natural resources. While all of these technological changes occur, cyberwars will be conducted to

control knowledge. But at some point, the limits to Earth's natural resources will drive warfare. These resources will be basic—food, water, and air—as well as energy generation, distribution, and transmission to run it all.

Joseph Coates, Forecaster

The Singularity is mentioned several times, and it is completely overblown in its potential. The Singularity is spun out of Kurzweill's mind as if he were afraid of dyng, and all the future developments will occur to allow his brain to be downloaded to a robot. Hence the magic 40 years at which he sees that happening. More substantively, he commits an error that would embarrass a freshman in a computer science program. He confuses quantity with quality. Specifically he sees dramatic increase in computer capacity. Whether he is correct or the extent to which he is correct is irrevelant to the error he makes, which is to assume that mere capacity will allow for the "duplication" of the human brain. Neither in his book nor in his articles does he reveal any deep understanding of current progress in brain science, or the enormous problems confronted in neuroscience of understanding the kinds of subjects that he bases his singularity on. I think it is a serious mistake to crank up your client's interest and concern about the Singularity, when I see It as only one small step above hokum.

Dr. Jonathan Czarnecki—Instructor, Naval Postgraduate School

I believe the issue will be, in the long run, irrelevant. Here is why.

We know from our anthropological and archeological research that humans tended to compartmentalize warfare from economics and society when it was of interest to at least one of the warring parties to desire the existing economic and societal goods of the other(s.) Your report, and the comments of your participants, indicate that not only is the trend of collapsing warfare into the economy and society continuing, it is accelerating. When parties engaged in warfare do not place value on their opponents' being or resources, only a Clausewitzian ideal war can result. Yes, I am referring to nothing less than Armageddon.

Now hold on before you write me off as a crank. The End Day(s) I write of are virtual. The only reason the Internet continues now is that the general and vast majority of users believe that it is safe, and they are secure. If someone can undercut those feelings and beliefs, the Internet dissolves.

As we more and more "open source" warfare, physically and virtually, we encourage others who do not like us and do not want us to live to take more and more drastic action against our growing preeminence in virtual reality.

Pose this question to your participants. Tomorrow, when they wake up, there is no Internet. Anything connected to or dependent on the (unclassified or NIPRNET) net is gone as if it never existed. It cannot be reconstructed. What now?

Dr. William E. Halal

A fine study, but I wonder if the urgency of cybercrime and cyberwarfare is fully appreciated? Our studies on the TechCast Project suggest that this is not something that will happen in 10 or 20 years—it is happening now. Our experts forecast that 3 to 4 billion people will use the Internet, smart phones, laptops, PCs, and TV by 2015, roughly doubling present usage. This accelerating growth of electronic media is likely to increase the level of hacking, virus attacks, and other forms of cybercrime and cyber warfare dramatically over the next few years.

As others have noted throughout this report, existing systems like the Internet are not capable of handling these massive threats, and the world is increasingly fragile, so unusually strong protections are needed. The most obvious need is to support rapid deployment of the "Second Internet" that is intended to solve the security problem. But even the most brilliant security systems may not be able to manage these threats by themselves, so political programs are also needed to bring alienated nations and groups into the fold where cohesive relationships discourage attacks.

Maj. Matthew J. Lennox—Instructor, American Politics, Policy, and Strategy, U.S. Military Academy, West Point

Early thoughts and perspective:

The material provided presents thoughtful trends in cyber warfare, but also generates several questions with respect to second and third order effects of these attacks on several levels: politically, socially, economically, etc. Some of these questions are listed below:

- What effect do these attacks have on the legitimacy and continuity of governments, and how do standing government policies play into the threat of cyber warfare?
- Will the increased connectivity enhance or degrade our civil society?
- Will the availability of information increase the effects of relative deprivation, especially as expectations rise and resources diminish?
- Despite trends that seem to forecast economic strength, can cyber manipulation exaggerate that public's loss of confidence in the government and economy?
- How do we preserve the basic foundations (liberty, equality, privacy …) of a democracy?
- How will the lack of privacy impact people?
- Could cyber attacks diminish the legitimacy of the ballot box?
- With the nation-state no longer the keeper of information, how will nation-states respond? Will states cede more power to regional or global organizations? Who is accountable?
- Will the state try to dominate the information sphere and lose some of its democratic nature?

One of the issues we wrestled with was the nature of cyber warfare: is it its own form of warfare? Despite isolated examples and proof of concept tests depicting cyber warfare as capable of causing physical damage, it seems that cyber warfare, at this point, is

predominantly a combat multiplier (1). The primary focus of the attacks mentioned in the paper is to disrupt. However if the attacking elements mission is to destroy confidence for its own sake, cyber warfare alone may be capable of achieving the goal.

Expanding the scope of non-nation-state actors:

In most of the "Implications for Information Warfare and Operations" sections, the report rightly focuses on the role of nation-states and their cyberwar capabilities, but non-state actors are also developing capabilities in this art of warfare. The report acknowledges the capabilities of terrorist organizations focused on achieving religious, cultural, and political ends (p.56), but may overlook organizations whose primary aim is to make money. Organized crime syndicates can operate as both criminals (digitally holding banks / corporations hostage) and electronic-guns for hire. They are apparently willing to work for cash or large batches (1000s) of credit card numbers. There may be some economic or even political destabilizing effects from these criminal / mercenary type organizations (2).

Concern about security and the trend toward self employment or new small businesses:

The report examines the trend toward self employment and small businesses surviving industry consolidation, but does not address the second order affects or risks associated with current government policy to work with some off-the-shelf-equipment and smaller parts brokers. A recent *Business Week* article highlighted a Pentagon move to buy parts from companies that may offer lower prices than the original equipment manufacturers or authorized retailers. This shift was further affected by "federal affirmative-action goals [that] further encouraged the military to favor suppliers that qualify as 'disadvantaged.'". A second order effect or unintended consequence of these policies is that the parts brokers, some of which were never vetted, can potentially import compromised parts (computer chips with backdoor access) from possible competitor nations or adversaries (3).

Government loss of legitimacy:

One of the government's responsibilities is to provide security / services for its people. In the event that several highly publicized service disruptions (loss of power, loss of water …) occur via cyber attack, the public may lose confidence in their government's ability to provide that service or security. This could lead the population to seek their security / services from other sources, undermining the role and legitimacy of the government and its leaders.

The paper also evaluates the population's perspective on privacy or the safe-guarding of personal information. The paper addresses this within the framework of a security versus liberty issue. Another perspective may be that compromised information kept or managed by the state (loss of digital medical records or other personally identifiable information on a grand scale) agitates one or more socio-economic classes. Essentially, what happens if someone makes a deliberate effort to place stress on the seams of our

society? This could occur if lower economic classes receive (manipulated?) information that upper-classes are receiving a perceived difference in standard / quality of care, i.e. when the government has to decide where and how to distribute a new, limited quantity drug to the public, in a relatively short period of time.

Water:

With respect to water, the paper focuses on global and regional shortages of clean, consumable water. Water delivery is at times controlled by Supervisor Control and Data Acquisition systems, like the electric grid. Thus, it can be susceptible to service disruptions as a function of network attacks. (Consider the 400+ mile California aqueduct system, where water flows both as a function of gravity and pumping stations.)

Robust to failure versus robust to attack:

The paper mentions fault tolerant infrastructure that can self-correct and limit cascading impacts (p. 38). Ideally, being robust to faults will help when under attack. However, there is a difference between being robust to failure and robust to attack. Predictive models assume that failures are random and thus less likely, on an absolute basis, to affect highly connected nodes. Attackers, on the other hand, have the ability to focus attacks on highly connected nodes, thus disrupting large portions of networks. Thus, a network that is robust to failure is not necessarily robust to attack (4.).

Example: Within the electric grid there are generating stations, transmission lines, substations, distribution lines, transformers, and monitoring equipment. Assuming each component has an equal likelihood of failing, failures would occur most frequently (on an absolute basis) on the most common items within the grid, probably the distribution lines and transformers. A failure of either of these two items would most likely not have the impact that losing a power generation station, transmission line, or substation would have. Attackers on the other hand would specifically target the power generation and transmission capabilities because of the nature (as a highly connected node in the network) in order to have a larger impact and cause a cascading failure throughout the system.

Endnotes:

1.) Combat Multiplier: Supporting and subsidiary means that significantly increase the relative combat strength (power) of a force while actual force ratios remain constant. Examples of combat multipliers are economizing in one area to mass in another, leadership, unit morale, surprise, deception, battlefield information, camouflage, electronic warfare, psychological operations, terrain reinforcement, smoke, and indirect fires. (See also combat power.) See FM 100-5.

See “Russian Hackers Target U.S., Europe for Profit and Politics”

2.) See "Russian Hackers Target U.S., Europe for Profit and Politics"

3.) See "Dangerous Fakes," *BusinessWeek*, October 13, 2008, p. 34

4.) See Barabasi, "Linked: How Everything Is Connected to Everything Else and What It Means"

_____

John W. Peterson—Managing Director, The Strategy Augmentation Group

On the Evolution of Cyberwar

'A Neanderthal Attempts to Interpret a Glimpse into a Possible Future'

WORKING DEFINITION: Today, at all levels of strategy (political, strategic, operational and tactical), the information technology revolution is driving substantive changes in postmodern battlespaces. The ever-improving accuracy, lethality, and destructiveness of weapon systems juxtapose against multiple dimensions (space, air, surface, subsurface, cyberspace, and temporal) and the ever increasing breadth and depth of the battlespaces have combined to increase the value of information to a point where its dominance may provide discernable advantage at all levels of engagement to its practitioners.

Cyberwar extends much further than the Internet (and its evolving successors) and involves electronically deceiving, blinding, jamming, overloading and/or intruding into an adversary's (or potential adversary's) information and communications networks, including command and control infrastructures; intelligence collection, processing and distribution infrastructures; and underlying communications and positioning technologies (including but not necessarily limited to IFF (identify friend-or-foe) and tracking "smart" unmanned systems.)

Cyberwar also involves conducting operations according to information-related principles including establishing dominance in the veracity and accuracy of information and knowledge and maintaining that dominance while denying similar information and knowledge, veracity, and accuracy to an adversary. As such, it has broad ramifications for organization and doctrine including a need for networked structures (which requires greater decentralization of command and control) and non-kinetic engagements including psychological operations and the undermining of both an adversary's morale and its willingness to resist. Cyber capabilities also provide greater understanding of the 'bigger' picture, minimizing the fog of war, and enhancing management of the complexity that is conflict.

In summary then, Cyberwar is an extension of the traditional importance of obtaining information, converting it into knowledge and leveraging that knowledge down the kill-chain more quickly than an adversary. It requires superior command, control,

communication and intelligence technologies and a willingness to find, feel, fix, surprise, and deceive the an enemy. Hierarchical command and control gives way battlespace/killchain management. In civilian terms (and cynically postulated), Cyberwar simplifies to: 'leveraging knowledge to minimize the capital and labor investment expended to 'close with' and kill or capture an adversary and undermine its will and ability to resist.'

CONTEXT: Just beyond the nexus of the second and third Tofflerian waves is a technology driven future. Of particular interest during the next three decades will be the roles of bioinformatics and biomimetrics in the next long wave business cycle. 'Progress' will result from the exploitation and manipulation of molecular genetics enabled by nanotechnology, quantum processing, bio-computing, and ubiquitous sensing. In parallel, the Grover algorithm (quantum processing) massively reduces the computational requirements for elaborate attempts at synthesis, including DNA sequencing. Cross species molecular breeding and augmented human capabilities will be an ultimate result. Such efforts will be paralleled by machine calculations and neuroinformatics with processing speeds on the order of 30 million billion calculations per second (by 2020). Behavior modeling will offer predictive value as communicating micro-sensors (both active and passive) feed data repositories and macro models and simulations. Non-invasive transcranial projection will allow both active and passive behavior modification. Nano-enabled robotic technology will begin to redefine human roles in commercial (particularly in the agriculture and manufacturing) sectors, social activities, and conflict amelioration. This will ultimately cause radical changes in the cohesiveness, structures, and definition of national and regional 'interests'.

The rate of technology diffusion in the next three decades is a significant unknown. In the United States, the current generation of decision makers has been shaped by the recent past and is sustained by what was the 'then' usual. Reflected is an economic 'shake-out' accompanied by decades of miserly restraint in funding new technology based systems and in fundamental research. Forward-looking development has essentially been ceded to Universities and private laboratories. Big business commercial investment has almost all been limited to those incremental technologies that perform traditional tasks both faster *and* cheaper. Demands for new technologies to reshape things are pent-up, but the current generation of executives has been trained to cut budgets for incremental profit, not invest to reap future returns. Unlike elsewhere on the globe, breakthrough technologies in the U.S. have become fewer and further between.

This mindset is problematic because it still takes five-to-ten years to develop significant new technology based solutions and place them into effective use. Current information and communication technologies were typically designed to allow for incremental improvements for half their anticipated use-life. Translated, that means many American companies will still be attempting to leverage the information technology of the year 2000 in the world of 2030 (beware of Commercial-Off-The-Shelf (COTS) – we may place ourselves at the mercy of first players with new and better solutions!) By 2020 the growing influence of transnational companies and the real-time capabilities of their

private armies (including short term mercenary rentals) will greatly compromise slow moving bureaucratic attempts at establishing static defensive measures with obsolescent technologies. (Cyber defensive measures, although necessary, are doomed to be reactive and, as a result, will never keep pace with offensive capabilities. Eventually even the best cyber defenses will be ineffective against a determined attack by capable adversaries.)

Additionally, bytes do not, and will not replace bullets. Cyberwar technologies are both very powerful tools and very vulnerable assets. Essentially, they are an inverted pyramid, balanced on its point of electronic components. By 2030, a single converted/shielded airliner carrying an electromagnetic pulse (emp) generator powered by a zero point energy module, orbiting above the homeland, could create an emp wave sufficient to take down almost all U.S. based C4I capabilities.

SOME CRITICAL VECTORS IN INFORMATION TECHNOLOGY: Current COTS solutions are primarily adaptable to adversarial situational awareness; early warning and dynamic training applications. In order to break the incremental mind-set, emerging information technology solutions will need to find widespread applications in government and the military as well as in science and engineering first. The end game for users will be the creation of the means for timely access to accurate but inexpensive information for use at all levels. The differentiating value of information will reside less in its existence and more in its analysis and integration. Macro drivers will include:

- Persistent monitoring/surveillance (augmented by coherent change detection). Commercially this would include manufacturing, computer-aided design and computer-aided manufacturing (i.e., of microcircuits with feature sizes less than 1 micron, including the tools, dimensional inspection and measuring systems with capability to control the manufacture of microcircuits.) Currently evolving is a functional hierarchical extension that progresses through virtual prototyping, data visualization, visually coupled systems, and virtual reality systems, including all the elements of sophisticated modeling and simulation. Similar capabilities would be reflected in parallel cross-multifunctional military activities including strategy, war planning, theater management, battle planning, kill-chain management, control, and follow-up including but not limited to conception/notion, assessing, locating, planning, targeting, tracking, engaging, assessing and following-up; similar capabilities would extend into most other sectors over time.

- Machine fusion (i.e., organization and prioritization of pertinent information including filtering unnecessary data), this includes high-performance computing, exceeding 20 million billion calculations, roughly equivalent to one human mind by late 2010 and then to the equivalent of a town full of human minds by 2030 (on a personal computer). General-purpose digital processing equipment, including computers, digital signal processors and array/vector processors with composite theoretical performance including dynamic scene generation, real time capability, characterization of dynamic scenes, texturing, etc.; as well as information relating same to effectiveness of learning. Included are intelligent

systems, including robotics, systems, and software that assess and reveal adversaries tactics, limitations, vulnerabilities, etc.

- Tele-everything, the delivery of near real time (NRT) information from many multiple sources/sensors to authorized decision makers; enabling real-time communication among analysts, decision makers, and commanders. This includes both new optical and new mobile networking and switching architectures capable of speeds in excess of 100 terabits/sec. High-speed, low latency distributed intelligent switching systems and network operating systems capable of automatic redistribution of machine intelligence functions to adapt optimally to new conditions and requirements. Software, including machine generated symbolic manipulation that enables 'silicon,' bio, and quantum processors to implement applications, validate data, and provide systems superiority (100 percent functional predictability with high confidence (> 99 percent), high reliability (~ 100 percent); immunity (< 1 error in 1012 transactions); external > cryptographic data (including quantum) integrity with low probability of error (< 10-9; internal-detect-fix < 1 operational cycle.)

- Massive amounts of supporting data accessible by all with a need to know. This includes immersion, i.e., a real human systems interface with dynamic scene generation algorithms; feedback algorithms; smoothing algorithms for variable resolution, orientation stereo displays including data visualization applications. Conversion of complex numerical simulations or learning experiments into a graphical images, using computers and visually coupled systems to achieve user immersion field of vision >70 degrees vertical and >120 degrees horizontal and direct trans-cranial access to 'other' human bio sensors, brain portals and the brain itself, including radio frequency, magnetic, etc.

- Accurate, projected information within protected open access systems. This includes large complex systems modeling and simulations including climatologic modeling, and battle mapping. Also included would be real-time sensor performance prediction, weather prediction, oceanographic modeling, accurate air and ground tasking patterns, congestion, transport and resupply predictions, resource allocation and delivery priority, etc.

- Information Security – encryption (including quantum using Shor's algorithms), subspace communication (inadequately defined as 'readable' geographically diffused phase entangled quantum objects reflecting actual data), digital signature techniques to ensure veracity of access, artificial intelligence functions, intrusion detection, and countering techniques.

THE THREAT SPECTUM: Deliberate cyber threats can be categorized consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001. These threats include: national

governments, terrorists, industrial spies, organized crime groups, activists, and hackers, but have been somewhat paraphrased for brevity.

- **National Governments:** National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and loss of life and extensive infrastructure disruption. Among the array of cyber threats currently identified, it is government-sponsored programs that are expected to develop capabilities with the future prospect of causing widespread, long-duration damage to critical U.S. infrastructures. The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or defended critical infrastructures. For the next two or three decades, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to substantively attack critical infrastructures. Sub-objectives are thought to be espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to undermine the US economy, counter force capability if attacked by the U.S., and preemptive capability to weaken the ability of the U.S. to launch full scale attacks.

- **Terrorists:** Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to undermine national security, create mass casualties, weaken the U.S. economy, and create fear while undermining public morale and confidence. Terrorists may also use phishing schemes or spyware/malware in order to generate funds or gather sensitive information. By 2030 substantial terrorist cyber threats will have emerged as a more technically competent generation enters the ranks.

- **Industrial Spies, Organized Crime Groups, and Private Armies**: Corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent. Their goals are profit-based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and to gain access and blackmail affected targets using potential public exposure as a threat.

- **Disenchanted/Activists: This grouping** forms a subset of politically active hackers that includes individuals and groups with motives to undermine policies and interests. They pose a medium-level threat of carrying out isolated but potentially damaging attacks. Most international forms of these groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their causes.

- **Hackers:** Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, individually they pose

minimal threats of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as defended networks or infrastructure elements. Even fewer are thought to have the motivation to do so. Hackers break into networks for the thrill or the challenge and to claim bragging rights within the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use.

The large worldwide population of hackers poses a relatively high threat of an isolated, short duration incident. None-the-less they could cause a brief disruption and serious damage, including extensive property damage and loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack. In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure. Although the numbers that follow are essentially meaningless (the assumptions are fuzzy at best) they do begin to reveal the magnitude of the potential threats:

- 2030 World population: 8,000,000,000
- Psychopaths (1 in 100): —> 80,000,000
- Sociopaths (1 in 25): —> 320,000,000
- Loners (1 in 4): —> 2,000,000,000

It is currently thought that about one third of the world's population has access to computers and the Internet, either at work, home or cyber cafes (or local equivalents.) If that number reaches fifty percent by 2030, one might estimate that there could be as many as 40 million psychopaths and 160 million sociopaths with the potential capability to bring hurt on national infrastructures or other critical entities. If only ten percent of those 200 million have the skills and tradecraft necessary to be particularly effective, that leaves a potential of 20 million attackers. This number does not include loners and those 'normal folks' in service to their national governments or transnational companies, private armies, or motivated by other tribal, religious, or ideological loyalties. The potential for cyber attacks is both massive and real, and if multiple attacks were both coordinated and cascaded, the effects would be overwhelming. Most sobering, however, the Cyberwar genie is already out of the bottle!

SUMMARY: In the emergent interdependent global economy, Americans will be ill equipped by their public educations to understand, leverage, and maintain the capabilities inherent in a new complex and technologically grounded infrastructure. The challenge, i.e., to support and defend the constitution and promote the American way of life, will not be to deal with constrained access to resources, but to quickly understand new contexts (including new science), foster new ideas, and leverage new solutions. The enabling externalities, the new keys to technology diffusion, will occur at the

nexuses of dramatic changes in capability, 'need' and new science. The externalities will include but certainly not be limited to:

- The slide of the United States from superpower to same as any other 'run of the mill' nation [Currently, $300 billion trade deficits; more than 30 other nations are currently devoting more of their GDP to Research; failure of the K-12 U.S. education system; and resultant disparate technical abilities coming on line in the US labor force; and 70 percent of the potential military service manpower pool unfit for service.]

- Selected global moral ambiguity concerning human experimentation will see the introduction of the first augmented humans and, as a result, a 'forever change' in intellectual development and in warfare. Additionally, quantum teleportation (molecules by 2030), will allow the targeting of individuals (neural pathways, blood vessels, bionic enhancements) as technological solutions, including robotics and adaptive artificial intelligence, are sought to provide parity and continuity in leadership, analysis, and intellectual applications.

- Leaner national defense budgets and an accelerating shift in defense requirements to defend against 'non-explosive' strategies of social disruption (behavior) as opposed to the destruction of resources (Newtonian physics and munitions). This will accelerate as information gathering by technical means 'go black' (inexpensive and ubiquitous quantum encryption and non-electro-magnetic spectrum (subspace) signaling). Related venues include the quantum everything [imaging, optics, holography, nucleonics, teleportation, etc] to replace obsolete electronic means and capabilities.

- Spending to adopt solutions incorporating advanced traditional Newtonian physics versus more robust quantum realities. Gating factors will be the varying abilities of transnational decision makers/corporations/political leaders to recognize resultant capabilities. Competing technologies will translate into global ubiquity of capability. Critical differentiators become information access (observation), interpretation (orientation), decision models (decision), and execution (action) [i.e., Boyd's OODA loop and the Meder data ontology]. The winner (least damaged survivor) will be determined by which actor is first able to gather and assess the information necessary to get inside an adversary's decision cycles.

Open warfare remains a knife fight with straight razors inside a crowded elevator. Everyone is going to get cut, but the 'winner' and some of the innocent may well survive. Offensive cyberwar capabilities remain offensive tools that, at least for a couple of decades, hold the promise of preparation and the potential for preemption. And this is in spite of the stark new realities of the changed world we will have to face.

Peterson, item 2:

Targets: USA

Potential Hostile Over-arching Strategies

Description: Simultaneous explosion of multiple sets of thermonuclear devices (mines) placed along both coasts by non-metallic unmanned submersibles off loaded from merchant vessels mid ocean and masquerading as pods of migrating whales. Explosions ignite ocean (methyl and ethyl) nitrates, nitrites and methane. Resulting tsunamis create ocean front property in Arizona, Nevada, Utah, Missouri and Arkansas

Strategy Level: Political (Over-arching)

Primary Target: Inhabitants and infrastructure of the United States

Probability by 2030: Moderate—complexity requires sponsorship by nuclear capable hostile government and high risk of discovery and direct military response

Impacts: Extremely High

Casualties: Millions (up to 80% of the coastal populations)

Consequences: Destruction of the United States of America

Description: Influence the American electorate to elect passive isolationist government with no interest in 'Pax Americana' or the global spread of democracy. Declaration of unilateral ceasefire by the multitude of terrorist organizations and rogue states in late 2014. No terrorist incidents in 2015 or prior to the 2016 elections as terrorists withdraw to the global hinterlands, reorganize, refit, retrain and plan. Ceasefire maintained until new administration budget reductions and force reductions are well under way. Then all Hell breaks loose.

Strategy Level: Political (Over-arching)

Primary Target: United States National Elections in 2016

Probability by 2030: Moderate to Low. Complexity requires participation by many fragmented groups with different agendas and no real central command and control.

Impacts: High

Casualties: Initially, only National Security and Military Budgets.

Consequences: Undermining of global co-operation and an inability of the US to fulfill standing treaty obligations.

Description: Undermine the advantages and military prowess of the western democracies with the creation of a UN standing army. Nominally meant to standardize and regulate policing and peacekeeping operations but with the authority to regulate military treaties, policies, practices, and allowable technologies. UN mandated, enforceable in the Hague (world court.)

Strategy Level: Political (Over-arching)

Primary Target: Western military prowess and technology

Probability by 2030: Moderate to Low; requires approval of too many disparate nations.

Impacts: Moderate.

Casualties: Sovereignty of the Western democracies.

Consequences: Collapse of the world order and dominance by non-democratic states.

Description: Simultaneous dirty bomb explosions in Mexicali, Chihuahua, Monterrey, Durango, and Ensenada; refugee columns head north in response to (false) rumors of U.N. and U.S. resettlement camps offering abundant food, water, and medical services in Southern California and Arizona. Weaponized anthrax, small pox, plague, and gas gangrene spores released from "news" helicopters overflying the columns. As refugee

disaster mounts on U.S. borders, conventional explosive detonations create multiple breaches in aqueducts supplying runoff/snow melt from Sierra Madre and Rocky Mountains.

Strategy Level: Political.

Primary Target: Inhabitants and infrastructure of the Southwest.

Probability by 2030: Low; technology complexity requires sponsorship by hostile government(s) and high risk of discovery and direct military response.

Impacts: High.

Casualties: Tens (if not hundreds) of thousands from disease, starvation, and thirst; additional thousands as Mexican criminal elements force down borders and attempt to assert dominance over local American law enforcement. Open warfare on the streets of the southwestern United States.

Consequences: Politically destabilize the region, foster anti-Hispanic violence, and implode the over- stretched American infrastructure.

Strategic Targets

Description: Coordinated effort to destroy petroleum reserves with introduction of latent petroleum eating (transgenic) life forms into the national petroleum reserves resulting in massive contamination. Replacement needs create market shortages and drive-up prices

Strategy Level: Strategic.

Primary Target: United States strategic petroleum reserves

Probability by 2030: Moderate to Low; complexity requires very advanced transgenic research and development.

Impacts: Moderate.

Casualties: Curtailed capabilities and rationing for civilians. All military and civilian mechanical systems.

Consequences: Economic crises and operational capability curtailment as "systems" become dependent on spot oil markets to keep both military and civilian vehicles moving.

Description: Swarm (50 or more) of toy aerial improvised explosive devices released from pleasure craft gathered to watch departure of U.S. nuclear aircraft carrier (first in

San Diego, CA, and less than a week later, in Naples, Italy. Each micro model (toy) aircraft carrying equivalent of ½ pound of C4 and ¼ pound of weaponized anthrax, small pox, plague or gas gangrene spores . Models flown into superstructure, flight decks, and open hanger bays.

Strategy Level: Strategic.

Primary Target: United States aircraft carriers

Probability by 2030: Moderate to High.

Impacts: Moderate.

Casualties: Scores of crew casualties as secondary explosions and fires cause hundreds of millions of dollars in aircraft, radar and C4I equipment damage.

Consequences: Global Operational capability curtailment; ships unfit for service for up to three months while undergoing decontamination and repairs.

Description: Undermine military technology advancement by Identifying leading researchers (DARPA awards and patent filings); and perpetrating coordinated geographically dispersed attacks by suicide hit squads.

Strategy Level: Strategic.

Primary Target: Intellectual Drivers of Advanced Military Critical Technologies.

Probability by 2030: Moderate.

Impacts: Moderate.

Casualties: Dozens.

Consequences: Lengthy delays in delivery of military critical technologies.

Description: Create (or steal) transgenic animal and plant developments (persistent self-replicating transgenic microorganisms that secrete toxins) capable of contaminating large aquifers. Pump into targeted aquifer(s) from multiple dispersed home well systems.

Strategy Level: Strategic.

Primary Target: Aquifers in areas with critical defense production facilities.

Probability by 2030: Moderate.

Impacts: Moderate.

Casualties: Hundreds

Consequences: Major migrations of defense workers and their families, resulting in shut-downs of production lines and massive stranding of defense industry capital.

Operational Targets

Description: U.S. deployed microsatellite sensor apparently momentarily dazzled by laser. Because each microsatellite in the special-purpose constellation, for reasons of cost and weight, had but a single processor, the “dazzling” was actually an upload of a self-replicating avatar. The avatar installed itself in the processor’s buffer and was not sent forward in the data stream as content. It became part of the call header in the next communication transmission. It thereby gained access to the secure communications network where it established itself in additional communications processors, created trapdoors and opened access to the networks. It continued to replicate itself and eventually started randomly adding single bits to transmission error checks. Before long, the transmission networks were choked with messages determined to be in error state.

Strategy Level: Operational.

Primary Target: C4I networks.

Probability by 2030: Moderate.

Impacts: High.

Casualties: ?

Consequences: Inert American C4I Networks and loss of operational and tactical advantage.

Description: Periodically, night shift worker dumps thermos full of natural biological contaminant; i.e., Raccoon roundworm (*Baylisascaris procyonis*) or specifically developed transgenic microorganism spores (that remain inert until ingested by humans) into military ration packs.

Strategy Level: Operational.

Primary Target: Combat arms personnel.

Probability by 2030: Moderate.

Impacts: Moderate.

Casualties: Scores die, virtually all exposed require hospitalization and recuperation.

Consequences: Less than ready force structure; the point of the spear dulled.

Description: Military unit commanders identified; particularly those about to deploy (active, Reserve and Guard), and become victims of random geographically dispersed attacks by suicide hit squads.

Strategy Level: Operational.

Primary Target: Field grade military leaders.

Probability by 2030: High.

Impacts: Low.

Casualties: Scores.

Consequences: Degraded command, control, and unit leadership.

Tactical Targets

Description: In different cities in different parts of the country, series of multiple sustained toy aerial (and/or mobile ground) Improvised explosive device micro models, carrying equivalent of 1 pound of enhanced C4, randomly guided into vehicles during morning rush hour. Priority targets include school buses, police vehicles, and first responders.

Strategy Level: Tactical.

Primary Target: Vehicular traffic.

Probability by 2030: High.

Impacts: Moderate.

Casualties: Perhaps a dozen per city per attack.

Consequences: Disrupted transportation and creation of fear amongst the public and first responders.

Description: Simultaneous “visits” by terrorists dressed as firemen to Roman Catholic elementary schools in twelve different towns across the US. Upon entering the schools the terrorists enter nearest classroom, shoot the teacher, teaching assistant and male students with silenced .22 cal pistol. Terrorists spray the faces of the girls with sulfuric acid from what appeared to be a fire extinguisher. Attacks last less than ten minutes.

Terrorist egress successfully in all attacks except Austin, Texas, where three passers-by, hearing the screams of the children and seeing the armed men depart, open fire with their personal firearms. Autopsies later reveal 37 rounds in the bodies of the terrorists.

Strategy Level: Tactical.

Primary Target: The “innocents.”

Probability by 2030: High.

Impacts: Low.

Casualties: Scores.

Consequences: Fear, terror, random harm, demonstrate government’s impotence (inability to protect and serve.)

Description: Multiple terrorists place (the “old night-watchman thermos full of contamination trick”) persistent, self-replicating nanites or other pathogens that don’t present until ingested, in national brands of pregnancy vitamins and/or infant formula and/or fruit juices/baby food.

Strategy Level: Tactical.

Primary Target: Infants and families.

Probability by 2030: High.

Impacts: Moderate.

Casualties: Hundreds.

Consequences: Create fear, undermine faith in government’s ability to protect.

Description: Sustained series of non-nuclear EMP attacks from small trucks and delivery vans on data centers and major banking locations. System shut-down causes cash shortages. No credit cards; consumers face fuel, food, medical and gas shortages.

Strategy Level: Tactical.

Primary Target: Banking system.

Probability by 2030: High.

Impacts: Moderate.

Casualties: Finance system.

Consequences: Creation of black market mentality and tax resistant economy.

Bahukutumbi Raman—Additional Secretary (Ret'd.), Cabinet Secretariat, Government of India; Director, Institute For Topical Studies, Chennai

I have read the Executive Summary as well as the other documents sent by you with great fascination. Instead of giving point-by-point comments, I will give some general comments and leave it to you to decide what to do with them.

(a). India has terrorism of various hues—separatist, ethnic, ideological (Maoist), and jihadi (indigenous as well as originating from Pakistan and Bangladesh). Till 2007, only the jihadi terrorists originating from the Pakistan-Afghanistan region had shown a worrisome interest in using the Internet for operational purposes—such as propaganda, communications, motivation, training, data-mining, and disruption. The interest of other terrorist groups in the Internet remained confined to propaganda and psy-war and communications. They did not show any interest in the use of the Internet for disruption purposes.

(b). Jihadi terrorists operating in the Pakistan-Afghanistan region, including Al Qaeda, have been exhibiting an increasing mastery of the use of the Internet for propaganda, communications, motivation, recruitment, and training, but one has not seen any confirmed instance of their using or attempting to use the Internet for disruption purposes.

(c). Neither Pakistan nor Afghanistan has a large reservoir of IT-savvy anti-Western Muslims. India has a reservoir, but it cannot as yet be described as large. So too, the Pakistani and Indian Muslim diaspora in the West. Al Qaeda and pro-Al Qaeda organisations are focusing on them for the recruitment of their future IT warriors. The Indian Mujahideen has come to notice for recruiting at least three, but they were used for primitive purposes such as sending claims of responsibility without being traced back.

(d). Indian Muslims are technically less qualified than the rest of the population, but better educated and qualified than the Muslims in most of the Islamic world. They have the same access to IT education as a person of any other religion and the same job opportunity. As Al Qaeda and pro-Al Qaeda organisations start looking for recruits with a capability for disruption, they are likely to depend increasingly on the IT-savvy Muslims of India and the Indian and Pakistani Muslim diaspora in the West.

(e). How to disrupt their efforts at such recruitment? That is a question, which would the need the attention of the intelligence agencies of India and the West.

(f). All Islamic fundamentalist organisations—including the Taliban—have realised the importance of IT. The curricula of most madrasas exclude physical sciences, western philosophy, logic, etc., but include training in the use of computers, which are seen as

an asset for waging a jihad. In the 1990s, I had contributed to the quarterly journal of the United Service Institution of India, based in New Delhi, two articles on likely future threats from “microchip moles” and the computer as a “weapon of mass disruption.” These threats have not yet materialised, but it is only a question of time before they do. A weapon of mass destruction requires qualified manpower, financial resources, and a place to test away from the attention of the intelligence agencies. A weapon of mass disruption requires only qualified manpower and limited financial resources. This is a weapon which can be launched from anywhere. In most cases, the intelligence agencies will become aware of one’s capability in the field only after one has used it and not before.

(g). State-sponsored cyber war, that is, the use of lone wolf cyber warriors by States for achieving their intelligence-collection and disruption objectives, is a threat, which is already staring us in the face. Deniability is strong in the case of state-sponsored cyber warriors. Protective technology has to keep ahead of technology, which lends itself to disruptive uses. Is it doing so?

I am attaching an article written by me on October 8, 2008.

INDIA AS POSSIBLE WEB OF CYBER TERRORISM : INTERNATIONAL TERRORISM MONITOR—PAPER NO. 45

1. Many terrorism experts have been concerned since 9/11 that if there is an act of terrorism involving nuclear material, it will most probably originate from Pakistan. Hence, their worries about the security of Pakistan’s nuclear arsenal and about the possibility of radicalised Pakistani scientists helping Al Qaeda or pro-Al Qaeda organisations.

2. Is there a similar danger of an act of cyber terrorism, seeking to damage or destroy critical infrastructure, emanating from India because of the availability of qualified information technology experts in the Indian Muslim community? This question is likely to occupy the attention of the terrorism experts following the announcement by the Mumbai Police on October 6, 2008, of the arrest of 20 suspected members of the so-called Indian Mujahideen (IM), who had played a role in the serial blasts in Ahmedabad on July 26, 2008, in the abortive attempt to organise similar blasts in Surat the next day and in the serial blasts in New Delhi on September 13, 2008.

3. Among those arrested are four IT-savvy members of the IM, who had played a role in sending the E-mail messages in the name of the IM before and after the Ahmedabad blasts and before the New Delhi blasts by hacking into Wi-fi networks in Mumbai and Navin Mumbai. These are:

- Mohammed Mansoor Asgar Peerbhoy aka Munawar aka Mannu. A 31-year-old resident of Pune, who was reportedly working for Yahoo, India, on an annual salary of Rs. 19 lakhs (US $45,000).
- Mubin Kadar Shaikh, a 24-year-old graduate of computer science from Pune.

- Asif Bashir Shaikh, a 22-year-old mechanical engineer from Pune. In addition to helping in sending the E-mail messages, he also reportedly played a role in planting 18 Improvised Explosive Devices (IEDs) in Surat, all of which failed to explode.
- Mohammed Ismail Chaudhary, a 28-year-old computer mechanic, who is also suspected to have helped in planting the IEDs in Surat.

4. Peerbhoy is reported to have joined the IM while he was studying Arabic in Pune's Quran Foundation, which seems to have served as a favourite recruiting ground for jihadi terrorism. The U.S. intelligence agencies would be interested to know that he had allegedly visited the U.S. twice in recent months. Did he go on his own or in connection with Yahoo's work? This is not clear.

5. Pune as an important recruiting centre for jihadi terrorism has come out of the investigation made so far by the Mumbai Police. One would recall with interest that Abu Zubaidah, the Palestinian, who was supposedly No.3 in Al Qaeda, was also reported to have studied computer science in Pune before crossing over into Pakistan and joining Al Qaeda. He was arrested in the house of a cadre of the Lashkar-e-Toiba (LET) in Faislabad in Pakistani Punjab in March, 2002, and taken to the Guantanamo Bay detention centre in Cuba by the U.S. intelligence. He was considered an IT expert of Al Qaeda.

6. Peerbhoy has been projected as self-radicalised during a visit to Saudi Arabia for Haj. Despite this, certain questions need to be gone into thoroughly—were he and others self-radicalised or radicalised by Al Qaeda, which would welcome more IT experts? Were they recruits or volunteers as a result of their self-radicalisation? Were they working only for the IM or were they also helping Al Qaeda and other pro-Al Qaeda organisations?

7. Their capabilities as demonstrated till now are rather primitive relating to sending E-mail messages through hacked networks. Many young students can do this. Did they have any other capability of an ominous nature?

8. If the reports that Peerbhoy had visited the U.S. twice in recent months are correct, it shows that he had a valid visa for the U.S., which he had probably got on the recommendation of Yahoo. It also shows that the Federal Bureau of Investigation (FBI) had no adverse information on him. Otherwise, the U.S. would not have issued a visa to him. If he had managed to get himself transferred to one of the Yahoo offices in the U.S. or in West Europe, Al Qaeda would have had a wonderful cyber sleeping cell in the West. Why did he weaken the possibility of his getting posted to the West one day by helping the IM in doing a simple job of communications, which did not require much expertise?

9. These and other questions of a similar nature require to be gone into in great detail, if necessary, by enlisting the help of the cyber experts of the U.S. intelligence.

T. Irene Sanders, executive director of the Washington Center for Complexity and Public Policy

Cyber Security

One of the lessons we are learning from the current economic crisis is that individual financial institutions do not operate in isolation; they are part of a dynamic, nonlinear, and interconnected global system. Linear cause-effect thinking and final solution responses do not work. The same can be said of cyber security.

If we think of cyber security only as network security—protecting engineered systems of hardware and software and shoring them up when a breach occurs, then our foresight is diminished and our strategies will be short-sighted and ineffective over time. If instead we use insights from complex systems research to think of cyber security from a broader perspective—as a complex adaptive system evolving within a changing big-picture context—then we will have better insight about the present and foresight about the future.

Complexity science provides a new *theory-driven* framework for thinking about, understanding, and influencing the dynamics of complex systems, issues, and emerging situations. Understanding the global cyber security landscape or ecosystem from this perspective will enhance our ability to protect the country's critical information infrastructure as it is evolving, identify new threats and opportunities as they are emerging, and respond effectively to ongoing changes in the larger environment, before a crisis arises.

Stated simply, complexity arises in situations where an increasing number of independent variables begin interacting in interdependent and unpredictable ways. Complexity science represents a growing body of interdisciplinary knowledge about the structure, behavior, and dynamics of change in a specific category of complex systems known as *complex adaptive systems.*

Most of the world is comprised of complex adaptive systems—open evolutionary systems that are continuously processing, and incorporating or adapting to new information/feedback from the larger environment. A rain forest, traffic, the stock market, our immune systems, a business, a society, the United Nations, and the World Wide Web are examples of complex adaptive systems. These types of systems whether physical, biological, or social share a significant number of characteristics including diversity, emergence (local system interactions create global behavior or patterns), self-organization, nonlinearity, and sensitivity to initial conditions; i.e., small changes can create big results at some point in the future.

President Obama has made cyber security a major focus of his Homeland Security agenda. As he and his administration work to fulfill their intention "to keep the homeland secure from 21st century threats" and to secure our overseas operations, they will need to establish a coherent and ongoing interdisciplinary process based on complex

systems thinking. Figure 1 is designed to illustrate the complex evolving worldwide cyber context and some of the issues and trends related to cyber security. It also includes several complexity-based questions that need to be considered on a regular basis.

Figure 1: The evolving global cyber context.

From Figure 1, it's obvious that there are clusters of trends, issues, and questions that are important to pay attention to. Many sub-issues will fit under these cluster headings.

Trend Clusters

- **Changing Nature of Attacks (a macro trend)**
- **Changes in Technology**

  (grid, cloud, supernets)

- **Law Enforcement & Criminal Prosecution**

  cyber espionage (government and corporate)

- **R&D**
- **Standards and Protocols**
- **Cyber Alert Systems**
- **More of the world coming online (a macro trend)**

  Ways in which Internet is used for work, social contact, politics

- **Education about cyber issues & safety**

  Public and Policy-makers

- **Economies worldwide**

  Will cyber war be used to influence conflicts over resources like food and water?

- **Geo-techno-politics**

  Where are our servers?

From this beginning list of clusters, it would be easy to identify additional issues, concerns, trends, or questions that need to be added. An interdisciplinary group working through this type of exercise would quickly have greater insight about the present situation including our vulnerabilities to attack and greater foresight about the future including the novel ways in which cyber war could be successfully waged against the U.S.

It would also be important for the group to have an overview on complexity science and what scientists have learned about the nature and uses of complexity. From such a process a coherent and integrated strategic cyber security plan could be developed, implemented and revised in response to ongoing changes in the cyber security environment.

Nico van Klaveren

It is not an optimistic review of the situation—past, now. and future. There are few solutions offered—and those that are are not reachable in the present political/social environment.

A question in my mind was “What are we trying to achieve?” It is obvious that “national security” or “protecting the western civilization” can only be a short-term goal. We have to look at the global situation.

A lot of talk about “singularity”—here the point where “computers” attain self- sufficiency and control our lives? Well, if that is the scenario we better get our societies organized because it will be the starting point for at the “singularity.”

Finally, education is the key. Science and technology are important to keep “ahead of the others.” And, our main problem—particularly in the U.S.—is that we do not have enough young people motivated to pursue these fields. However, the main “education” we need is an awareness of where we are and where we want to go in, say, philosophical terms. We are doing even a worse job preparing our youth to think along these ways.

55 Trends for Cyberwar

POPULATION TRENDS

1. The world's population will grow to 9.2 billion by 2050.

Early versions of this report predicted that the world's population would double by 2050, and population growth has proceeded almost exactly on schedule. However, even this estimate may be too low. According to the Center for Strategic and International Studies, most official projections underestimate both fertility and future gains in longevity. Unfortunately, the greatest fertility is found in those countries least able to support their existing people. Populations will triple in the Palestinian Territories and Niger between 2000 and 2050 and will more than double in Yemen, Angola, the Democratic Republic of Congo, and Uganda. In contrast, populations in most developed countries are stable or declining. The United States is a prominent exception.

Assessment: Demographic trends such as this are among the easiest to recognize and most difficult to derail. Barring a global plague or nuclear war—wildcard possibilities that cannot be predicted with any validity—there is little chance that the population forecast for 2050 will err on the low side.

Implications: Rapid population growth in the United States compared with its industrialized competitors will reinforce American domination of the global economy, as the European Union falls to third place behind the United States and China.

To meet human nutritional needs over the next forty years, global agriculture will have to supply as much food as has been produced during all of human history.

Unless fertility in the developed lands climbs dramatically, either would-be retirees will have to remain on the job, or the industrialized nations will have to encourage even more immigration from the developing world. The third alternative is a sharp economic contraction and lower living standards.

A fourth alternative is the widespread automation of service jobs as well as manufacturing, to accomplish the work needed to support accustomed living standards. However, this requires development of a means other than wages to distribute wealth and to provide both a living income and a fulfilling occupation for workers and would-be workers displaced by machines and software.

Barring enforcement of strict immigration controls, rapid migration will continue from the Southern Hemisphere to the North, and especially from former colonies to Europe. A growing percentage of job applicants in the United States and Europe will be recent immigrants from developing countries.

Implications for Information Warfare and Operations: The world population's growth is less significant than where those people are concentrated—upwards of 1.1 billion in India and over 1.3 billion in China. India already has the largest supply of English-speaking scientists, engineers, physicians, and technicians in the world. China soon could have the largest population of technically trained workers on the planet; 40 percent of its college students major in engineering. All this suggests that Asia will be

home to an enormous number of technically sophisticated people. A small fraction—but probably a very large raw number—will have the skills needed for information warfare and operations.

Beijing already has stated its goal of being able to fight and win "wars under conditions of informatization." Its theoreticians have put considerable work into methods of attacking, defending, and exploiting computer networks, while many incidents of "hacker"-style penetration of American commercial, government, and military networks have been traced to China. Under these circumstances, that country's population represents a mil-tech asset that the United States cannot hope to match, save by superior education and training.

We rate this a high-impact trend, given China's stated intentions, with a 95 percent probability that these implications will prove correct.

Expert Comments:

Hoffman — Here again a bit of detail is needed to uncover potential implications. More than 80 percent of the population growth will occur in Asia and Africa. The educational **systems** in the latter will not support the advancement of knowledge workers to any degree, and could be swamped by poor governance, lack of services, and chronic disorder. Many places in Asia will experience some of the same downsides of large population growth without adequate governance, services, and education.

Pearson — Increase in population comes with increase in number of malicious people too, as well as more benign people to tackle problems. The increase in overall human resource is probably more of an asset than a threat overall.

Sowa — HIGH PROBABILITY: Cyberwarfare in the 21st Century will target infrastructure to gain strategic and tactical advantage, trade and intellectual secrets, and enhance passive monitoring to gain power and money. The lack of technically-sophisticated westerners poses one of the largest threats here through 2030 as the U.S. ages rapidly.

Steele — Disproportionate segments of world's population growth in the developing world will produce a widening gap between developed and developing worlds. This produces environments of anomie and alienation as a breeding ground for terrorist ideology. Yet, a growing proportion of the world's population (including the developing world) is gaining primary and secondary school equivalent education. The diffusion of cyber systems in the developing world increases opportunity for global cyber war.

2. People are living longer throughout most of the world.

The U.N. reports that "population is living longer" throughout the world, except in Russia and sub-Saharan Africa. Each generation lives longer and remains healthier than the last. Since the beginning of the twentieth century, every generation in the United States

has lived three years longer than the previous one. An 80-year-old in 1950 could expect 6.5 more years of life; today's 80-year-olds are likely to survive 8.5 more years. Life expectancy in Australia, Japan, and Switzerland is now over 75 years for males and over 80 for females. A major reason for this improvement is the development of new pharmaceuticals and medical technologies that are making it possible to prevent or cure diseases that would have been fatal to earlier generations. Medical advances that slow the fundamental process of aging now seem to be within reach. (This is an extremely controversial issue within the medical community, but we believe the evidence appears quite strong.) Such treatments could well help today's younger generations live routinely beyond the century mark.

Assessment: See the Assessment for Trend 1.

Implications: Global demand for products and services aimed at the elderly will grow quickly in the immediate future, but this trend may pass as geriatric medicine improves the health of the elderly.

Developed countries may face social instability as a result of competition for resources between retirement-age Boomers and their working-age children and grandchildren. At the present rate of growth, public spending on retirement benefits in the United States and other developed countries could be one fourth of GDP by 2050, even as the number of workers available to support each retiree declines sharply.

Barring dramatic advances in geriatric medicine, the cost of health care is destined to skyrocket throughout the developed lands. This could create the long-expected crisis in health-care financing and delivery. However, dramatic advances in geriatric medicine are all but inevitable. Paying the high cost of new drugs, technologies, and therapies will reduce the overall cost of caring for patients who otherwise would have suffered from disorders delayed, eased, or cured by such advances. In the end, these reductions will offset many of the expected increases, leaving the average health-care bill in the developed lands much lower than the doomsayers predict.

Any practical extension of the human life span will prolong health as well and will reduce the incidence of late-life disorders such as cancer, heart disease, arthritis, and probably Alzheimer's disease. This would dramatically reduce demand for products and services in the senior market, at least in the developed world. FI believes this development is nearer than even many researchers expect.

Healthier aging in the developed world may offer new hope to the world's poorer, sicker lands. Faced with declining growth in their pharmaceutical industries, western nations—and particularly the United States—are likely to subsidize research and treatment for diseases that burden the poor countries of Africa and Asia. This will give those lands their first real prospects for economic growth and improved quality of life.

Implications for Information Warfare and Operations: In the developed lands, aging represents the opportunity to accumulate wealth, and the elderly are the wealthiest

segment of society. Healthier lifestyles and better geriatric medicine also will help to ensure that seniors remain a potent force in society much later in life than was the case in previous generations. At the same time, the Baby Boom generation lacks the technological sophistication of the Dot-coms and Millennials. They also may have less practice at filtering reliable information from dross, a necessary skill for those who make their intellectual home on the Internet. Indeed, they may lack the energy or interest needed to bypass assertions that, however incorrect, fit comfortably with their prejudices. All these factors could make older, but still active, people a particularly suitable target for disinformation campaigns. They may be relatively likely both to accept falsehood and to wield political influence on that defective basis.

However, other factors also are at work. Older Americans in particular are much less dependent on the Internet than the young. Disruption of information flow will have a less direct affect on their lives. Loss of banking networks would have at least as great an impact on them as on those of working age. Loss of the Internet would not touch them nearly as personally.

Also, in the United States, we may see an education effect. The Baby Boom generation grew up in a time when critical thinking was an effective component of the classroom experience. To the extent that the American school system has neglected this facet of education, the benefits of being Net-savvy may be somewhat offset for the post-Boomer generations.

The last three presidential election cycles offer excellent case studies of the ways in which the impact of information warfare varies by generation. The willingness to accept information uncritically led to the successful “swift-boating” of John Kerry. The rapid rise and downfall of Sarah Palin via intense blogging campaigns, and the mobilization of the young to vote also show the potential and subtleties of the information “warfare.”

This trend will have a medium to low impact on information warfare and operations due to the competing effects, but its probability stands at 100 percent.

Expert Comments:

Callanan — Advances in information and communication technology have clearly meant that the mobilisation of all sorts of groups pursuing a wide variety of causes is both easier and cheaper. Virtual networking can be reasonably expected to lead to a proliferation of a larger number of smaller “specialised” extremist groups, some of whom may spend as much time vying with each other as much as anything. Nevertheless, this presents the security community with the daunting task of fronting up to a far more diffuse threat than until now.

In terms of cybercrime, one can expect the main focus of the intelligence community to be around a three-pronged approach: detection; interception and intervention to undermine the technology infrastructure of extremist groups; and influencing.

Sowa — Generational differences will cause exploitive tensions. The lack of critical thinking skills will increase the capability to recruit potential cyberwarriors from the Western youth.

3. The elderly population is growing dramatically throughout the world.

Worldwide, the elderly (age 65 and over) numbered 440 million and represented 6 percent of the global population in 2002. Their numbers will nearly double by 2020 (and form nearly 9 percent of the total population) and more than triple by 2050 (becoming nearly 17 percent.) In the developed world, people age 60 and over made up one-fifth of the population in 2000 and will grow to one-third in the next half century. Throughout the developed world, population growth is fastest among the elderly. In the United States, there are 4.2 million people age 85 and up. By 2050, there will be 19.3 million. In Europe, the United States, and Japan, the aged also form the wealthiest segment of society.

Assessment: Again, this is a demographic trend, difficult to derail and unlikely to change while the massive Baby Boom generation remains on the scene.

Implications: Not counting immigration, the ratio of working-age people to retirees needing their support will drop dramatically in the United States, Germany, Italy, Russia, Japan, and other countries. This represents a burden on national economies that will be difficult to sustain under current medical and social security systems.

In the next two to three decades, shortages of health workers will loom large in “aging vulnerable” countries. The United States in particular will need at least twice as many physicians specializing in geriatrics as its current 9,000, as well as half a million more nurses by 2020.

Suburban communities are likely to face a growing demand for social services such as senior day-care, public transportation, and other programs for the elderly. This will place a growing strain on local government budgets.

In the developing countries, where the elderly have traditionally relied on their children for support, this system will begin to break down as middle-aged “children” find themselves still supporting their parents while anticipating their own retirement.

Among the developed lands, Japan already is at greatest risk for this kind of decay. With fertility below the replacement level, it will need 17 million foreigners by 2050 to maintain the population it had in 2005. However, Japanese culture is extremely resistant to immigration. This conflict between need and inclination can be expected to produce severe societal stresses in the coming decades.

Implications for Information Warfare and Operations: See Trend 2.

Expert Comments:

Pearson — Possibility of intergenerational conflict due to pensions/increased power of older votes/older people clogging up the streets etc, young may come to deeply resent older people and refuse to pay, or emigrate to younger parts of the world, leaving some developed countries as retirement zones, with low wealth, high taxes, and only the old and useless living there.

Sowa — Generational realities are creating the need for even faster integration of cyber-network infrastructures into daily lives globally. This further integration — like the self-regulated financial sector — poses major management and counter-cyber-threat problems that need to be addressed.

4. Mass migration is redistributing the world's population.

There are nearly 100 million international migrant workers in the world, according to the United Nations. About 30 million live in Europe, 20 million in Africa, and 18 million in North America. These figures include only the workers themselves, not their dependents. About 4 million people immigrated permanently to the countries of the Organization for Economic Cooperation and Development in 2005, 10.4 percent more than the year before. Immigration to Western Europe from Eastern Europe, North Africa, the Middle East, and the Indian subcontinent continues despite controls enacted in the wake of terrorist attacks. Immigration is quickly changing the ethnic composition of the U.S. population. By 2050, the number of Latinos in the U.S. will double, to 24.5 percent of the population.

Assessment: As native workforces shrink in most industrialized lands, economic opportunities will draw people from the developing world to the developed in growing numbers. Thus, this trend will continue for at least the next generation.

Implications: Impoverished migrants will place a growing strain on social-security systems in the industrialized countries of Europe and North America. Similar problems will continue to afflict the urban infrastructures of China and India. Remittances from migrants to their native lands are helping to relieve poverty in many developing countries. Globally, these payments exceeded US$230 billion in 2005, according to the World Bank.

Significant backlashes against foreign migrants, such as the skinhead movement in Europe, will be seen more frequently in the years ahead. They will appear even in the most peaceful lands. For example, in Scandinavia, resentment against foreign workers is strong, in part because they can return to their native lands after three years of employment and collect a pension equal to the minimum wage for the rest of their lives.

• Since the terrorist attacks of September 11, 2001, and the rail bombings in London and Madrid, the large number of Muslim immigrants in Britain, France, and other European lands has inspired suspicion, and some persecution.

• Unfortunately, suspicion is to some extent justified. A tiny minority of Muslim immigrants has proved to be linked to terrorist groups, and some have plotted or carried out terrorist attacks. So have native-born Muslims and converts to Islam.

Implications for Information Warfare and Operations: Barring enactment of strict immigration controls, rapid migration will continue from the southern hemisphere to the northern, and especially from former colonies to Europe. A growing percentage of job applicants in the recipient lands will be recent immigrants from developing countries, at least a few of which have significant technical bases. This offers both the source countries and non-state actors within them the opportunity to place technologically sophisticated personnel in potential target countries, in positions where they would have access to critical systems. Additionally, cultural isolation will provide "safe pockets" of society that will prove difficult to penetrate for humint.

There may also be a modest flow of senior personnel in the other direction, particularly to offshore branches of American and European companies. This could provide the industrialized countries with a few opportunities to place their own people in the developing lands.

Probability is 65 percent; impact is medium. As immigrants gain financial stability in their new homes, the incentive to continue as "terrorists" may be significantly diminished.

Expert Comments:

Ayers — The U.S. government has been warned by many (including converts from Islam) about the potential for infiltration and subversion, which could easily extend into the cyberzone. Indications of at least physical infiltration have already been reported in open source material (see Daniel Pipes' The West's Islamist infiltrators," *The Jerusalem Post* [18 August 2008] and Audrey Hudson's "'Cyber' gang targeted U.S. facilities," *The Washington Times* [6 July 2007].)

Cyber-espionage against Western nations has been noted as originating from locations such as Russia and China—both countries with long-running histories of physical infiltration. (See for example Christopher Hope's "Britain under attack from cyber foreign security terrorists, report warns," *The Daily Telegraph* [8 August 2008] and Jeanne Meserve's "International hackers going after U.S. networks," CNN [20 Oct 2007].) There is little doubt that countries engaging in traditional espionage would attempt to recruit insiders with access to sensitive computer systems.

Forster — A major risk here is the repatriation of terrorists from Iraq and Afghanistan to their native lands. Networked via communication technologies, these individuals and groups become de-stabilizing influences.

Pearson — As above, migration to get away from costs of older people is likely. Also seeing large re-migration, with people going "back" to their homelands or their ancestors' homelands, once economic situation becomes more favourable.

Snyder — International migration accounts for less than 2 percent of global population and has remained fairly constant over the past 15 years. The great bulk of mass population migration has been within national borders—primarily from rural to urban areas—which accounts for Trend 45.

Sowa — Technologically-adept migrants will be a major source of recruitment for cyber-warriors.

Tucker — Placing senior personnel from the developed countries in the developing lands may result in incidents of kidnapping people to extract corporate, technical, or trade specific information. Witness the case of Mexican kidnapping expert Felix Batista, who was likely abducted because of information or expertise he possessed about Mexican law enforcement and their anti-kidnapping strategies.

5. The physical culture and personal-health movements are improving health in much of the world, but they are far from universal.

During the 1990s, health in the United States improved by 1.5 percent annually, based on such measures as smoking prevalence, health-insurance coverage, infant mortality rates, and premature deaths. Since 2000, health improvement has slowed to just 0.2 percent a year, largely due to personal choices. The global obesity crisis is a significant countertrend to the physical-culture movement. Poor diet, physical inactivity, and associated obesity contribute to 47 percent of diseases and 60 percent of deaths worldwide. However, health consciousness is spreading to Europe. For example, a recent poll found that two-thirds of Britons now spend more to maintain a healthy lifestyle than they did a decade ago, and three out of four say they enjoy leading a healthy lifestyle. Unfortunately, much of the developing world still worries more about eating enough than about eating well.

Assessment: This trend always seems a case of two steps forward, at least one step back. We expect it to continue for at least the next generation.

Implications: As the nutrition and wellness movements spread, they will further improve the health of the elderly. Better health in later life will make us still more conscious of our appearance and physical condition. Thus, health clubs will continue to boom, and some will specialize in the needs of older fitness buffs.

Diet, fitness, stress control, and wellness programs will prosper. States will continue to mandate insurance coverage of mammography. By 2012, they will begin to require coverage of sigmoidoscopy and colonoscopy. By 2015,Congress will add coverage of many preventive-care activities to Medicare. The cost of health care for American Baby Boomers and their children could be much lower in later life than is now believed.

However, Asia faces an epidemic of cancer, heart disease, emphysema, and other chronic and fatal illnesses related to health habits. Like tobacco companies, producers of snack foods, liquor, and other unhealthy products will increasingly target markets in

developing countries where this trend has yet to be felt. Continuing health improvements in the industrialized world will be accompanied by a dramatic rise in heart disease, diabetes, cancer, and other such "lifestyle" disorders in the developing lands. Chronic diseases related to obesity burden national economies and could thwart economic progress in developing countries.

Implications for Information Warfare and Operations: This trend has no obvious applications to this subject, beyond its effect in expanding the senior population.

Expert Comments:

Pearson — Perhaps so, but these trends don't always stay fashionable, and cultures of laziness and don't care attitudes can also prevail sometimes. If economic stress reduces quality of life to point where people devalue life, conflict and terrorism might increase.

Snyder — I would propose that this trend be replaced by "falling birth rates," a widely-recognized demographic trend that is expected to constrain economic growth and to force greater reliance on information technology. Birth rates are falling world wide, especially in developed economies; Japan, Germany, and Russia are already losing population, and ALL developed countries—except the U.S.—are expected to experience shrinking populations within 10 years.

Sowa — Advances in remote monitoring and field service biotechnological instruments will greatly advance health and wellness and sustainabilities among warriors and special operations units that act independently.

Tucker — According to Eric G. Swedin (*THE FUTURIST*, May-June 2006) "The Chinese government has demonstrated that they are willing to intervene in the daily activities of their citizens when they have an incentive to do so.

"In 1995, China passed the Maternal and Infant Health Law, which required medical doctors to conduct prenatal testing and to advise couples with genetic diseases either to not marry or to consider sterilization. In cases where the couple has already conceived and genetic abnormalities in the fetus are suspected, the doctor is to advise abortion. While the law only compelled doctors to offer advice, not to compel abortions or compel that their marriage advice be followed, Western critics such as Frank Dikötter, director of the Contemporary China Institute at the School of Oriental and African Studies, the University of London, have pointed out that such advice in a one-party communist state is tantamount to a direct instruction.

"Some tradition-minded Chinese view birth defects as a sign of personal sin of the parents or a sign of sins committed by their ancestors. The intent of the 1995 Maternal and Infant Health Law is to remove birth defects from the population, since handicapped people are often condemned to a life of poverty because of the limited social safety net within China.

“It is not known how many potential births in China have been affected by this law. But for purposes of comparison, a study in the United States and Britain found that 3 percent to 5 percent of all live births have some sort of genetic disorder. It is reasonable to assume that a similar proportion of Chinese births have been prevented due to Chinese policies, though not all birth defects can at present be detected before birth.

“Bioethicists in the United States and elsewhere objected to the new Chinese law as a violation of fundamental human rights. The Chinese government, however, considers Western concepts of human rights to be no more than a weapon used by Western nations to rhetorically abuse the Chinese people. This is not to imply that there are not Chinese activists who advocate human rights—only that their point of view is officially suppressed.

“Given the current Chinese thinking in bioethics and the obvious intent of the Maternal and Infant Health Law, it is hard not to imagine the Chinese government taking the next step and actively promoting the creation of genetically engineered babies.”

Societal Trends

6. Societal values are changing rapidly.

Industrialization raises educational levels, changes attitudes toward authority, reduces fertility, alters gender roles, and encourages broader political participation. This process is just beginning throughout the developing world. Witness the growing literacy, declining birth rate, and broad voter turnout seen in India over the last decade. Developed societies increasingly take their cue from Generation X, the Dot-coms, and the Millennial generation, rather than the Baby Boomers who dominated the industrialized world’s thinking for most of four decades. Post-September 11 fear of terrorist attacks has led Americans to accept almost without comment security measures that their traditional love of privacy once would have made intolerable.

Assessment: This trend will continue for at least the next two decades in the industrialized lands and two generations in the developing world.

Implications: The growing influence of the post-BabyBoom generations will tend to homogenize basic attitudes throughout the world, because Generation Xers, Dot-coms, and especially the Millennials around the globe have more in common with each other than with their parents.

The highly polarized political environment that has plagued the United States since the 1980s will slowly moderate as results-oriented Generation Xers and Millennials begin to dominate the national dialogue.

As national security concerns have begun to lose their immediacy, family issues are regaining their significance in American society: long-term health care, day care, early childhood education, antidrug campaigns, and the environment.

Concerns about health care, education, and the environment helped to shape the 2008 presidential campaign.

Demand for greater accountability and transparency in business will be crucial for countries that wish to attract international investors.

Implications for Information Warfare and Operations: This trend has no obvious direct applications to the subject.

Expert Comments:

Pearson — Indeed, it might be said that values are on a random walk, uncoupled from the fixed reference point that religion once provided, and now influenced by whatever the current fad is. Witness the 180-degree change in attitudes towards gay rights in 25 years, or on abortion in 15 years, or on genetic modification in 10 years. Values changing rapidly can be a threat since any charismatic individual can achieve greater change and mobilise greater power in a much shorter time now.

Sowa — As societal values rapidly change, the motivating emphasis factors of society will change with them. Because of the global downturn a pause in the money chase, may make other cultural aspects more enticing. That could be a good thing, or a bad thing in regards to cyberwarfare.

Steele — Social organizational structures are emerging and morphing more rapidly than ever. However, while asymmetry is becoming normative human social systems are culturally lagged behind geometrically emerging cyber systems, networks, and socially constructed realities. This widening gap between human cultural evolution and societal cyber revolution produces system risk.

7. Privacy, once a defining right for Americans, is dying quickly.

Internet communications, a basic part of life for many people, are nearly impossible to protect against interception, and governments around the world are working to ensure their unfettered access to them. Corporate databases are collecting and marketing data on individual credit-worthiness, incomes, spending patterns, brand choices, medical conditions, and lifestyles. While privacy regulations bar distribution of much personal information in the European Union, restrictions in the United States are much weaker. Widespread surveillance of private individuals is technically feasible and economically viable, as tiny, powerful cameras now cost next to nothing. Increased surveillance has become socially acceptable in an age when many people fear terrorism and crime. Britons are caught on camera an estimated 300 times per day, Americans about 200.

Assessment: Pessimists could say that privacy already is a thing of the past; society is merely coming to recognize its loss. We believe that enough effective privacy survives outside the most authoritarian countries to justify noting its continued erosion. However, this trend could easily reach its logical conclusion within ten years.

Implications: In the future, privacy is likely to be defined, not by the ability to keep information truly secret, but by the legal power to restrict its distribution. Even this limited form of privacy will be eroded as both government and private organizations find legal justification for their interest in personal information. Once access is granted to any type of information, it is unlikely ever to be rescinded.

Most surveillance provisions of the USA Patriot Act will survive, even if the law itself is repealed or modified.

In the absence of a major terrorist event, most Americans will continue to consider privacy a "right," and privacy-related lawsuits are likely to proliferate as more people feel violated or inconvenienced by surveillance. However, courts will be unsympathetic to such suits for so long as conservative appointees dominate the bench.

In large and medium-size cities around the world, spaces that remain unwatched by video cameras will continue to shrink.

Growing numbers of companies, and even private citizens, will encrypt their computer data.

The number of criminal cases based on surveillance will grow rapidly in countries with the required technological sophistication and infrastructure.

Private citizens increasingly will use similar technologies to watch over government abuse, as in cases where bystanders have recorded police misconduct with their cell-phone cameras.

Implications for Information Warfare and Operations: This trend provides the opportunity to monitor and regulate information flows in ways that not long ago would have been considered intolerable. However, recent backlash to the Bush Administration's heavy-handed approach to counter-terrorism efforts, and especially to the erosion of personal privacy, may significantly alter the political landscape. Potential privacy safeguards may require much more sophisticated operational procedures to limit abuses and "blanket" authorizations, while still allowing carefully authorized and audited activities. Eliminating the ambiguity in regulations, even if more restrictive, will provide a better environment overall for operational efficiency.

The sacrifice of privacy to security concerns also may inspire a few technologically sophisticated dissidents to "hack" into computer systems that officials would prefer remained closed. This is a much smaller risk than those presented by China, Russia, and perhaps some Eastern European lands, but it should not be overlooked.

Probability is 95 percent; impact on information warfare, though not necessarily on society, is low. Increased restrictions will be balanced by a more clearly defined environment and rules of engagement.

Expert Comments:

Ayers — The death of privacy may be creating (or at least increasing) two segments of society that may or may not ultimately figure into a cyberwar scenario. One segment might be characterized by those who are caught up in virtual worlds, creating a variety of fantasy-lives, and thus a string of alter-egos or variations of the individuals' true personalities. The other social group could be comprised of those who withdraw from every electronically-driven level of society possible—essentially dropping out entirely.

Within the group that employs alternative actors in the virtual world, the morals or ethics that drive one element of an individual's personality (which is, perhaps the basis of an online character) may not be the same as those for another, separate element—and these distinct components may easily be "gamed" as multiple entities in the cyber domain. Who or what type of character each element becomes and what the resulting entities are capable of doing is almost anyone's guess. Participating in activities associated with cyberwar may not be out of the question when it comes one or more fragments of what is essentially a split personality. Considering the potentially large numbers of what might be classified as "cyber-misfits," almost anything is possible.

The group comprised of social dropouts are not necessarily out of the cyberwar scenario altogether. Their identities could easily be stolen and used surreptitiously for long periods of time. Alternatively, they could more easily be utilized in situations where a lack of an electronic trail (as well as an appreciation of cyber security) is a desirable trait–thus providing a "leg-up" in covert operations against a cyberwar adversary.

Kapinos — Surveillance of public spaces is becoming more commonplace and ubiquitous every year. On the plus side, a system of surveillance cameras can be a great boon to crime prevention, and the detection and interdiction of criminal activities (including terrorist acts.) With the further development of face-recognition software, these advantages could be enhanced to an even greater degree. However, a network of security cameras could certainly be vulnerable to hacking, either to disable the system at a key moment, or to plant "false image" data to confuse operators or hide activities. While they are quite useful, we need to guard against over-reliance on electronic security systems: any such system being potentially vulnerable to cyber-warfare.

Pearson — This will possibly become an electoral issue in some countries, but the timing of erosion of privacy means it is more likely to be eclipsed by other economic issues when it come to elections, so privacy is likely to be lost. Then it will be left for rebellion later to recover it.

Tucker — The hyper-surveillance scenario originally laid out by George Orwell in his seminal novel, *1984*, is certainly technologically possible today, but it's unlikely to manifest in precisely the way he described. The greatest threat to the future of privacy, I believe, is not any singular government entity. Rather it's millions of people with the means and the will to broadcast everything they say and do.

Our eagerness to “Twitter” and upload onto YouTube more and more of existence is what government surveillance expert Amitai Etzioni has called “the turn away from privateness.”

“Privateness is different from privacy,” he told me in conversation in 2006. “Even privacy advocates would agree that if you want to give up your privacy for any specific purpose, that’s certainly your privilege, and people do it all the time. The voluntary loss of privateness is definitely on the rise. People have become very willing to disclose things for a number of reasons—for 15 minutes’ fame on television, for convenience, for coupons and special marketing incentives, and so on.” Look closely and you can see privateness withering all around us.

At the Alton Towers amusement part in Staffordshire, England, visitors can ask for a radio frequency identification (RFID) band to wear around their wrist, “marking” them to the park-wide video-capture system. As the visitor goes about his or her day, camera footage is collected, catalogued, and digitally stored. When the person is ready to leave, he or she signals a computer to begin assembling the personalized footage, which is then transferred to a 30-minute DVD, available for purchase.

By 2010, the number of RFID tags manufactured every year is forecast by industry groups to rise to 33 billion annually. The Fitbit, a device the size of a hairclip, allows its wearer to monitor his or her exercise levels, calories, and sleep patterns and then upload that data to a publicly viewable database.

A Georgia Institute of Technology “smart home” watches its occupant cook so he or she doesn’t miss a step. The house monitors the person’s prescription drugs and alerts relatives and medical professionals when there’s an accident.

All these examples provide further evidence of a cultural shift away from privacy.

8. Time is becoming the world’s most precious commodity.

In the United States, workers spend about 10 percent more time on the job than they did a decade ago. European executives and non-unionized workers face the same trend. In Britain, an Ipsos MORI study found that 32 percent of people who had not visited a museum in the previous year reported having too little time to do so; in 1999, only 6 percent had cited that reason. China’s rapid economic development means its workers also are experiencing faster-paced and time-pressured lives. In a recent survey by the Chinese news portal Sina.com, 56 percent of respondents said they felt short of time. Technical workers and executives in India are beginning to report the same job-related stresses, particularly when they work on U.S. and European schedules.

Assessment: This trend is likely to grow as competitive pressures lead companies to demand ever greater productivity from their employees and as changing technologies add the need for lifelong study to the many commitments that compete for the average worker’s time. As it matures in the United States, it is likely to continue developing in

other parts of the world. It will not disappear until China and India reach modern post-industrial status, around 2050.

Implications: Time pressures will grow even more intense as companies squeeze even more productivity from their existing workforce rather than hiring new people in the face of the current global recession.

Stress-related problems affecting employee morale and wellness will continue to grow. Companies must help employees balance their time at work with their family lives and need for leisure. This may reduce short-term profits but will aid profitability in the long run.

As time for shopping continues to evaporate, Internet and mail-order marketers will have a growing advantage over traditional stores. That 64 percent said they were never late and were intolerant of other people's tardiness suggests a new cultural challenge to the traditional Chinese concept of a leisurely existence.

China, India, and other developing countries can expect consumer trends similar to those in the United States as workers seek out convenience foods, household help, and minor luxuries to compensate for their lack of leisure time.

Implications for Information Warfare and Operations: The forces underlying this trend will continue moving the world's work and record-keeping to networked computers as quickly as technology and budgets allow. This will make much information more vulnerable to unauthorized access. This hazard will be greatest for private corporations and civilian government departments, but many corporate computers will be connected to non-sensitive military networks. These in turn may give access to more critical systems.

Probability is 65 percent; impact is medium. Many vulnerabilities will be overwhelmed by the glut of meaningless or irrelevant information that will be collected and stored.

Expert Comments:

Pearson — Rejection of cash as the main motivator in life would change the balance of power between different social groups and even countries. However, I believe we will always have some people who are time-rich and cash poor and vice versa. Not everyone wants to rush, but we don't all want to slow down either.

Sowa — Cyber-networks and collaboration over networks will have the greatest impact over 90 percent of all business factors in increasing worldwide productivity over the next 20 years. Cyberwarriors will most-likely make use of this to access sensitive areas.

9. The women's equality movement is losing its significance, thanks largely to past successes.

According to some, though not all, studies, women have nearly achieved pay parity with men in the United States when factors such as educational level, responsibilities, and seniority are taken into account. Younger generations of women are better educated and are even more likely to be successful than their male peers. Generation Xers and Millennials are virtually gender-blind in the workplace, compared with older generations.

This is true even in societies such as India and Japan, which have long been male-dominated, though not yet in conservative Muslim lands.

Assessment: This trend is valid only in the developed lands. In the developing world, the movement toward women's equality is barely beginning. In the United States, the trend could be seen as complete, with women's equality now taken for granted and only mopping-up operations required to complete the process. However, we believe that the women's equality movement will continue to retain some importance, less with each passing year, until the gender-blind Generation X and Millennials accede to leadership in business and politics.

Implications: In most of the developed world, whatever careers remain relatively closed to women will open wide in the years ahead. Japan will remain some years behind the curve, owing to the strength of its traditionally male-dominated culture.

Women's increasing entrepreneurialism will allow the formation of entrenched "old girl" networks comparable to the men's relationships that once dominated business. The fraction of women entering the American labor force has leveled off in recent years. The percentage of female workers is likely to remain approximately stable until some force appears to begin a new trend.

Demand for child care, universal health coverage, and other family-oriented services will continue to grow, particularly in the United States, where national services have yet to develop. Over the next twenty years, American companies may increasingly follow the example of their counterparts in Europe, whose taxes pay for national daycare programs and other social services the United States lacks.

There is little sign of progress for women in much of the developing world. India is an exception, because growing literacy has given women the chance to earn income outside the home and, with it, gain value other than as wives and mothers.

Implications for Information Warfare and Operations: There are few, if any, implications for this field.

Expert Comments:

Pearson — This may be a little out of date. Most reducnancies in the U.K. due to the recession are of women, so women are losing power fast right now. Later, AI effects will favour women. Governments are always more interested in legislating against the symptoms of inequality rather than addressing the underlying causes, many of which

are often due to value differences. Women don't want the same things as men, so forcing equality in all spheres is counter-productive.

Sowa — Women are more likely to be used as cyberwarriors over the next 20 years, as they will be less likely to be stereotyped as a threat, yet the trend here indicates pretty much an equality with men — and some superiority in math and science.

Tucker — Wild card: The Western environmental movement and the international women's rights movements join forces to increase access to reproductive care around the world, to curb population growth and fertility. This exacerbates Muslim antagonism toward the West.

10. Despite some xenophobic reactions to immigrants, there is growing acceptance of diversity.

Migration is mixing disparate peoples and forcing them to find ways to coexist peacefully and productively. Because of this, the interaction of diverse cultures will continue to grow, both internationally and intra-nationally, throughout much of the world.

The Internet and other technologies promote long-distance communication and build links between distant, and disparate, people. The globalization of business is having a similar impact. However, in many countries there are powerful reactions against these changes. The growth of the German neonazi movement after unification in 1992 is one obvious example. American hostility toward undocumented aliens may be viewed as another.

Assessment: This trend applies most clearly to the West, where it will continue for as long as we can foresee. In other regions, including Japan and large parts of the Muslim world, it remains weak, if it exists at all.

Implications: Groups with highly varied customs, languages, and histories of necessity will develop ways to coexist peacefully. Nonetheless, local conflicts will continue to erupt in societies where xenophobia is common.

Companies will hire ever more minority workers and will be expected to adapt to their values and needs. Much of the burden of accommodating foreign-born residents will continue to fall on employers, who must make room for their languages and cultures in the workplace.

Public schools and libraries must find more effective ways to educate this future workforce.

Implications for Information Warfare and Operations: Where this trend fails, immigrants who find themselves disadvantaged and ostracized by the dominant society may be available for dissident activities. However, limited educational opportunities may prevent most potential recruits from engaging in information warfare.

Expert Comments:

Pearson — True, and risks reduce to some degree. However, tribalism is deeply rooted in human nature and acceptance is not always mutual, as we see with acceptance of Muslims into the west, who sometimes then fight against the host community. tribal conflicts will always re-appear in some form or another.

Snyder — Monocultures, including Japan, Germany, Korea and Russia, remain openly hostile to immigrants. Historically, resistance to immigration increases whenever domestic prosperity declines—including in the U.S., where Congress continues to reject employer appeals to increase H2B visa quotas. While immigration rates remain high in the U.S., U.K., Canada, and Australia, they have recently been curtailed by Austria, Denmark, Sweden and the Netherlands. I believe that Trend 11 is overly sanguine concerning the future acceptance of immigration, especially given the prospects for a prolonged global recession.

Sowa — Xenophobia and outcasts will continue to create an atmosphere of "victimization" that will in return build a larger base of potential cyberwarrior recruits.

Steele — Global cultural interactions will produce unexpected outcomes and potential challenges to global stability. Not only will continued intercultural synthesis increase, but non-nation-state combatants will be joined by cyber system combatants (in singularity engagement.) Some will be human controlled, some will be cyber system controlled (machines creating and controlling themselves.) Cyber-cyber engagement may rely on a cyber system's ability to "out-evolve" its cyber opponent. Literally, beyond human control.

11. Tourism, vacationing, and travel (especially international) continue to grow with each passing year.

International tourism grew by more than 6 percent in the first half of 2007, thanks in part to global prosperity. By 2020, international tourist arrivals have been expected to reach 1.6 billion annually, up from 842 million in 2006. By 2020, according to the World Trade Organization, 100 million Chinese will fan out across the globe, replacing Americans, Japanese, and Germans as the world's most numerous travelers. Some 50 million Indian tourists will join them. Given the current global recession, we believe these targets will be reached about three years late.

Assessment: Travel seems to be in the DNA of the middle and upper economic classes. This trend will continue so long as national economies continue to generate new prosperity for the formerly poor.

Implications: Travel will grow by at least 5 percent per year for the foreseeable future.

The tourism industry will create 3.3 million new jobs worldwide. Jobs dependent on tourism will comprise nearly 14 percent of the global workforce.

Direct employment will not grow quite as quickly, but it will be up 1.7 percent annually, to nearly 87.5 million jobs, while indirect employment will account for some 260 million jobs around the world.

This will bring major opportunities for national economies in Southeast Asia and Africa, where Chinese and Indian tourists can take quick, inexpensive vacations.

Implications for Information Warfare and Operations: Modern travel depends heavily on computers and communications systems that would be obvious targets for disruption. Air traffic control systems are particularly critical.

Travel in recent years has involved a growing risk of kidnapping, particularly in Latin America, parts of Africa, and some of the Muslim lands. Computer specialists traveling in those areas may need to take security precautions that are unlikely to occur to many mid-level corporate workers. The disappearance of a high-level network security technician while on vacation in Acapulco, for example, could have significant implications for his employer and its clients, potentially including government agencies.

Probability is 30 percent; impact is low unless air traffic control systems are compromised; in that case, it becomes high.

Expert Comments:

Forster — The increase in travel & tourism means that the impact of penetrating the air traffic control system in the United States or elsewhere, thereby allowing terrorist to crash planes and simply degrade the system's ability to manage its task, would have dire economic consequences as well as potentially causing a large loss of life.

Pearson — Some tourist hotspots will cap the numbers of visitors as global tourist numbers increase. Eventually, only the great and the good and rich can get access, leading to other peoplebeing limited to visiting replicas, or even VR replicas. Tourism will come with quotas, and be become part of future trade wars.

Sowa — Transportation and logistical cybersystems will remain a target that can and will be compromised by cyber-attacks. Travelers can turn into cyber-mules with RFID and other implantable technologies.

Steele — Uploading cyber information directly to humans and to AI systems, then instantaneously morphing this information in creative alternatives produces a virtual and instantaneous change environment. This will require cyber system (beyond human) thinking and symbiotic cyber-human relationships (as well as cyber-cyber relationships.)

Snyder — Since 2000, this trend has largely been the product of the sham prosperity created by the credit bubble and suppressed tax rates. In the coming period of scarce, expensive credit and rising taxation, Americans in particular will spend less on discretionary travel and more on home entertainment. Business travel declined by 5

percent to 10 percent during 2008, and corporate travel budgets are currently projected to decline by 15 percent to 30 percent in 2009.

Tucker — This again raises the prospect of kidnapping people for passwords. It also raises the prospect of people transmitting data from locales they believe are secure but that really are not.

12. Education and training are expanding throughout society and our lives.

Rapid changes in the job market and work-related technologies will require increased training for almost every worker, just as knowledge turnover in the professions requires continuous retraining and lifelong learning. Thus, a substantial portion of the labor force will be in job retraining programs at any moment. All of the fastest growing occupations require some form of advanced training and continuous updating of job skills. In the next 10 years, close to 10 million jobs will open up for professionals, executives, and technicians in the highly skilled service occupations. In order to give those who cannot attend their classes a chance to educate themselves, the Massachusetts Institute of Technology has put its entire curriculum on the Internet, including class notes, many texts, and sometimes videos of classroom lectures. Other institutions are following suit.

Assessment: This is another trend at the beginning of its life.

Implications: Over the next two decades, the growing demand for education and training is likely to transform our working lives and educational systems around the world. In order to keep up with growing demands for education, schools will train both children and adults around the clock.

The academic day will stretch to seven hours for children to enable students to compete with their peers in other countries, who already devote much more of their time to learning, with predictable results.

Adults will use much of their remaining free time to prepare for their next job. In knowledge-based economies, a region's growth prospects depend on its ability to generate and use innovation. This correlates roughly with the number of college-educated adults living there. Throughout the industrialized countries, this gives cities an advantage over rural and suburban areas. It is one reason upwardly mobile adults tend to move to the cities.

Skills are the most important factor in economic success today. Unfortunately, the people who need them most, the poor and the unemployed, cannot afford schooling and therefore are least able to obtain them. Helping people overcome this disadvantage is a natural role for government.

As the digital divide is erased and minority and low-income households buy computers and log onto the Internet, groups now disadvantaged will be increasingly able to educate and train themselves for high-tech careers.

Even the smallest businesses must learn to see employee training as an investment, rather than an expense. Motorola estimates that it reaps $30 in profits for each dollar it spends on training. Both management and employees must get used to the idea of lifelong learning. It will become a significant part of work life at all levels.

Implications for Information Warfare and Operations: Computer competence will spread rapidly in the next two decades, and the number of people with a basic understanding of network security will grow much more quickly than the number for whom this is a core skill. Some of these peripheral figures may have the curiosity or specific motives needed to develop significant proficiency in this field. Under the right circumstances, they could present threats to whatever networks capture their attention. Security training and implementation will become more commonplace and ultimately will provide more hardened networks and reduce social-engineering vulnerabilities.

Probability is 85 percent; impact is low. The impact of this trend has both positive and negative aspects, which will largely balance out.

Expert Comments:

Forster — Increased access to education and training inevitably leads to an increase in the number of people who have the mental capacity to use technology for evil as well as good. Controlling access to education is neither possible nor morally responsible; however, awareness of potential negatives is essential and the United States needs to take appropriate steps to increase science and technology education to maintain an ability to counter those who seek to harm.

Pearson — Education is environmentally damaging since it leads to higher wealth and higher environmental impact. It also creates a larger pool of people with the skillsets needed to make new weapons. We also need a large pool of people who are not so well educated to do the more menial jobs, since otherwise education can’t produce a better standard of living, since the costs of menial work increase due to shortage of labour. The margin for being educated is therefore lessened, leading to resentment of the system.

Snyder — To wage cyber warfare, we need cyber warriors! While college attendance in the U.S. is rising, enrollment in the physical sciences, engineering, math and computer technology all continue to fall, leading U.S. IT firms to establish all their new research facilities in Asia over the past five years.

13. Advanced communications technologies are changing the way we work and live.

Telecommuting is growing rapidly, thanks largely to e-mail and other high-tech forms of communication. About 80 percent of companies worldwide now have employees who work at home, up from 54 percent in 2003. The number of telecommuters in the United States reached an estimated 20 million in 2006.

However, Millennials already have abandoned e-mail for most purposes, instead using instant messaging and social-networking Web sites to communicate with their peers. These and other new technologies, such as podcasting, are building communities nearly as complex and involved as those existing wholly in the real world.

Assessment: Again, this trend has only just begun.

Implications: E-mail promised to speed business. Instead, it absorbs more time than busy executives can afford to lose. Expect the nascent reaction against e-mail to grow as many people eliminate mailing lists, demand precise e-communications rather than open-ended conversation, and schedule only brief periods for dealing with mail. Instant messaging is likely to be even more destructive of time for the under-thirty set.

However, e-mail is a major contributor to globalization and outsourcing, because it eliminates many of the obstacles of doing business across long distances and many time zones. Unfortunately, e-mail and other modern communications techniques also have made possible a variety of crimes, from online fraud to some forms of identity theft.

They also make it virtually impossible to retract ill-considered statements or embarrassing online activities. Once something exists on the Internet, it is all but immortal and nearly impossible to hide.

Implications for Information Warfare and Operations: This is one of the two or three critical trends that give information warfare and operations their significance.

All the benefits and evils of e-mail, instant messaging, computer networks, and other communications technologies emerge from this trend. As these facilities become more sophisticated—for example, as early cell phones have evolved into “smartphones,”—they become not only more powerful, but more susceptible to misuse or tampering.

As our institutions computerize their operations, they become more vulnerable to unauthorized access. As they redesign their operations to take advantage of the efficiencies computers offer, they also open them to disruption by technologically sophisticated adversaries.

Disruption need not be overt or easily detected. With manufacturing systems increasingly open to direct input from customers, it might be possible to reprogram CNC machine tools to deliver parts that were subtly out of spec—and to rework the specifications themselves so that the discrepancies would never be noticed. If the tampering were carried out with sufficient imagination and care on well-selected targets,

the products might conceivably pass inspection, yet fail in the field. This could have significant military implications.

While digitized transmission of critical information will be more commonplace—and more vulnerable—the proliferation of garbage, meaningless trivia, and spam, will increase exponentially as well. This may render identifying the “needle in the haystack” an impossible task. Additionally, sender authentication and encryption technologies may very well make all but the most dedicated, and well funded, attack vectors moot.

Probability is 85 percent; impact is medium. In the short term, usage growth will outpace technological and security advancements; in the long term, the impact will decline to low.

Expert Comments:

Callanan — Advances in information and communication technology have clearly meant that the mobilisation of all sorts of groups pursuing a wide variety of causes is both easier and cheaper. Virtual networking can be reasonably expected to lead to a proliferation of a larger number of smaller “specialised” extremist groups, some of whom may spend as much time vying with each other as much as anything. Nevertheless, this presents the security community with the daunting task of fronting up to a far more diffuse threat than until now.

In terms of cybercrime, one can expect the main focus of the intelligence community to be around a three-pronged approach: detection; interception and intervention to undermine the technology infrastructure of extremist groups; and influencing.

Coates — As everyone recognizes, the Internet is a mess, open to all kinds of uses, misuses, anti-social material, irksome intrusions from ads, identity theft, international swindles, and on and on. That has all come about because the Internet grew incrementally, through the work of bright to brilliant technologists, responding to a repeat theme, “We can do…. And you will make money.” No significant social, political, or regulatory group entered into the deliberations about “improvements.” The result is what we have is now. For these reasons, as well as the potential for national security interventions, and general hell raising, it is time to plan, design, and execute over the next five to seven years, a replacement for the Internet. If you have a polluted water supply, you don’t issue antibiotics, as a permanent policy. You fix the sewer system.

Forster — New communication technologies will further change the way conflict takes place. First, the ability to utilize communication technologies to achieve information superiority and dominance is essential. Second, denying others access to information will also be critical. Third, the ability to exploit information effectively will reduce the current asymmetrical differences between states and between states and non-state actors. For example, the size of the military will matter less than the ability to effectively use information to determine weaknesses and strike.

Kauffman — Non-nuclear EMP (electromagnetic pulse) bombs may be a serious danger for both military and civilian systems.

Detonated in the vicinity of the naval bases in Norfolk, VA; San Diego, CA; or Pearl Harbor, HA, an EMP bomb would permanently disable electronic equipment. Lost facilities would include communications with shore-based and distant commands; electronic communications between surface, undersea, air, and shore units; interior electronic communications on ships, aircraft, and shore stations; surface and air search radar, sonar, fathometers, and similar sensors; electronic navigation equipment. Weapons fire control capability would be reduced to manual control.

Detonated in lower Manhattan, EMP bombs would disable critical systems used by business and by public safety agencies. These include telephone, radio, and Internet communications; hospital diagnostic and therapy equipment; police, fire, and ambulance services; banks and storage facilities with electronic time locks; and of course the computers and communications equipment at the area's stock and futures exchanges.

LaDuke — Communication is shared comprehension and is integral to all knowledge interactions like learning, compiling, recollection, or knowledge creation. But more importantly it is at present the link between knowing and doing (performance) and it converts intent into action. For example, operational plans are communicated to guide tactical execution. In this sense cyber attacks are enabled by, or deterred by, communications. The signal of a threat is a signal of intention. Everything outside of the signal of threatening intention is either leading to this or noise.

Intelligence technology of the future will have three main fronts: 1) The traditional approach of communication interception, 2) Threatening intention detection through technology and 3) influence or persuasion to change intention.

Pearson — And also creating more vulnerabilities and more dependence. The "Age of magic," where only a few elite understand how stuff works, could lead to abuse of that power, just as the high priests held high power in old civilizations.

Snyder — In fact, communications has already begun to supplant travel—e.g., tele-commuting, virtual vacations, distance learning, and digital recreation.

Sowa — Impact is felt to be higher than the authors suggest.

Steele — Lack of personal and household preparation produces increased vulnerability to attack. Local and personal adaptation to rapidly changing cyber systems capabilities will be challenged. Whether combatants or civilians, cyber attack and rapid "Singularity Engagement" will produce rapidly changing social realities. The opportunity for creating "disinformation" and "false worlds" or consciousness may be instantaneous. In the current setting the local home failure to use cyber attack and antivirus software puts the

nation at risk. A desktop computer can easily be enlisted for use by an adversary—human or cyber.

As local households offload processes inside and outside their homes to cyber systems, micro level civilian attack by cyber warriors or cyber systems can bring down daily functions (heating, cooling, information transmission, etc.)

Cyber attack already the case at the local computer used level can only increase in Singularity engagement environment. External—internal distinctions between combatants become blurred.

Thomas — Psychological operations closely connected with social engineering: social engineering leads people to make certain selections on the Internet, and thereby can influence attitudes just as psyop does.

Impact of new media (blogs, ICQ, etc.) on cognitive processes and search for truth: spread of fake messages, altered images, YouTube videos are new methods of spreading news, sometimes to spread disinformation.

Tucker — These changes raise grave security concerns, and new vulnerabilities appear almost daily.

Researchers at the University of California, Berkeley, have discovered that by making highly accurate audio recordings of keyboard strokes they were able to reconstruct e-mail messages, retrieve data entered into a report, and recreate passwords typed into a secure Web site, essentially overhearing Internet conversations (Tucker, *THE FUTURIST*, Jan-Feb 2006.)

According to the researchers, once the system is trained, recovery of typed data becomes an elementary process, even in situations where the data was not in English, such as in the case of a code or password. After 20 learning cycles, the algorithm was able to accurately retrieve 69 percent of several 10-character passwords, 77 percent of eight-character passwords, and 90 percent of five-character passwords. The researchers were able to make the recordings using readily available over-the-counter equipment.

While this research is still very new, it raises new and novel concerns about the safety of information transmitted from supposedly “safe” locations, such as the business lounge of a highly-trafficked hotel.

Wildcard: Social networking is very popular among teens and puts them in direct contact with people around the world all the time almost immediately. People discover each other through common interests such as affinities for particular music bands, books, etc. It is possible to divine a great deal about these young people simply from their profiles. In the same way that adult technical workers who are in possession of sensitive information could be vulnerable to abduction, so their children could be as

well. Social networking makes it very easy to find, contact, and potentially lure the immediate family of technical workers into dangerous situations.

van Klaveren — I am presently involved in exploring virtual worlds and their possible applications. It is a certainty that "virtual worlds" will become a very important force in general life and especially in education. If one interacts with participants in Second Life—and have them tell you how much their real life ideas and attitudes are affected and modified by their participation, you can only conclude that virtual worlds will have a major effect on the way our cultures evolve. There are some very worrisome developments—but the potential for "good" is also tremendous.

Vogel — There are two technology-related areas that I believe that will impact—at least in the near- and mid-term—several trends listed in the paper, "55 Trends for Cyberwar:" cloud computing and Web 2.0 applications.

Cloud computing is a shorthand description of service-oriented computing. Namely, purchasing the computer infrastructure and hosted applications on an as-needed basis. The analogy often used is the use of electricity in our homes. When we want to light a room in our house we flip a switch and purchase the power to light the bulbs. When we have no need for the light, we flip the switch off and stop paying for the electricity usage.

Similarly, with cloud computing, there may be no need to purchase costly servers and other computer hardware. The hardware is purchased by another organization and we pay for what we use when we need it. The same applies to software applications. Rather than installing and maintaining the application on each of our PCs or servers, we rely on a third party to host and maintain the application and pay only when we access the application.

Access to infrastructure and applications is via the internet and to us the actual location of the hardware and software is "in the clouds." For example, when we purchase a book via Amazon.com, we have no concern whether the system we are accessing via the internet is in the US or a foreign country.

Gartner analysts Daryl Plummer and Thomas Bittman at the Emerging Technologies conference in Las Vegas, made the predication, "By 2012, 80 percent of Fortune 1000 companies will pay for some cloud computing service, and 30 percent of them will pay for cloud computing infrastructure."

Forrester analyst James Staten interviewed more than 30 companies and concluded that cloud computing has been "wildly popular" with small businesses but large companies have been skeptical.

The "popularity" of cloud computing will be driven by many factors including realistic budgetary considerations and security. Clearly, with IT budgets being reduced along with other corporate expenses, any way to save money and yet deliver needed services will be more attractive and gain favor. Security is another thing. Many companies and

government organizations are justifiability concerned with security-related issues associated with cloud computing. One expert from Gartner lists a number of security concerns, including

- Access control: Since sensitive data is processed outside the enterprise this brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.
- Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in.
- Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.
- Recovery. Even if you don't know where your data is, it is important to consider how data and service recovery will be addressed in case of disaster.

Some of these and other security concerns can be addressed in what is often referred to as "private clouds." Private clouds keep the resources within the enterprise while moving to a more sharable computing infrastructure. Basically, private clouds work in the same way as public cloud services, but are run by the enterprises.

The cybersecurity implications associated with cloud computing, whether a public or private cloud, are significant. As more companies and the government adopt cloud computing, they become more vulnerable to disruption and cyber attacks. This could result in disruption in services and the ability to rapidly access critical software applications.

Web 2.0 applications. With the wide-spread use of Facebook, blogs, and other social networking applications in our personal lives, government organizations are seeking similar capabilities for communicating and interacting with their stakeholders. While the technology exists, government must be cautious in implementing Web 2.0 capabilities until all major security concerns are addressed. Once the government permits interactive, two-way communications over government networks, the chance for cyber attacks dramatically increases.

GENERATIONAL & FAMILY TRENDS

14. Family structures are becoming more diverse.

In periods of economic difficulty, children and grandchildren move back in with parents and grandparents to save on living expenses. Many bring their own children with them. In the United States, one-third of Generation Xers have returned home at some point in their early lives. Among Millennials, the figure is even higher. The 2001 Census found that so-called "multigenerational households" are the fastest growing group in the United States. Yet the nuclear family also is rebounding in the United States, as Baby-

Boomer and Gen-X parents focus on their children and grandparents retain more independence and mobility.

Same-sex households also are gaining new acceptance. At least five American states now permit same-sex marriage or have enacted domestic-partnership laws that provide similar protections. In this, they join such countries as Denmark, Germany, the Czech Republic, the United Kingdom, and most recently Switzerland.

Many grandparents are raising their grandchildren because drugs and AIDS have left the middle generation either unable or unavailable to care for their children. This trend is strongest in sub-Saharan Africa, where there will be 25 million AIDS orphans by 2010.

Assessment: This trend will remain in effect for at least a generation in the United States, longer in the rest of the world.

Implications: Where many European countries have largely adjusted to this trend, the United States has not. Making that adjustment will be an important challenge for the next decades.

Tax and welfare policies need adjustment to cope with families in which heads of households are retired or unable to work. Policies also need modification for those who receive Social Security and work to support an extended family.

In the United States, the debates over homosexuality and the "decline of the family" will remain polarizing for the foreseeable future. The next debate is likely to focus on granting parental rights to more than two parents, as when a sperm or egg donor wants a role in the life of a child whose official parents are the recipients.

Implications for Information Warfare and Operations: This trend could eventually reduce some opportunities to blackmail employees in sensitive positions. Beyond this distant possibility, no significant implications appear.

Expert Comments:

Pearson — Potential route to "them" resentment, with some social groups or family structures benefiting at the expense of others. Lower feeling of belonging to "society" reduces strength of nation, and creates routes to undermine it.

Sowa — Employees will continue to be recruited and/or blackmailed in sensitive positions.

15. Young people place increasing importance on economic success, which they have come to expect.

Throughout the 1990s—effectively, their entire adult lives— Generation Xers, Dot-coms, and Millennials knew only good economic times. The economic downturn at the turn of

the century seemed to them a confusing aberration rather than a predictable part of the business cycle. The current global recession is a frightening wake-up call. Yet, most expect to see growing hardship on a national level, but they both want and expect prosperity for themselves. In the United States especially, most young people have high aspirations, but many lack the means to achieve them owing to high dropout rates and ineffective schools.

Assessment: This trend appeared with the Baby Boom generation and has strengthened with the later cohorts. It will be interesting to see what develops among the children of the Millennials, something we find difficult to predict with any confidence.

Implications: Disappointed ambitions will be a major source of political unrest in the United States and many other countries in the next two decades. Most of the other countries seriously affected by this trend will be in the developing world or will be host to large numbers of disadvantaged immigrants.

Entrepreneurialism will be a global trend, as members of Generation X and the Millennials throughout the world tend to share values. Generation X and Millennial entrepreneurs are largely responsible for the current economic growth in India and China, where they are becoming a major force in the Communist party. In India, the younger generations dress and think more like their American counterparts than their parents. In China, the democratic fervor that spawned Tiananmen Square has been replaced by capitalist entrepreneurialism.

If younger-generation workers find their ambitions thwarted, they will create growing pressure for economic and social reform. If change does not come fast enough in the developing world, disappointed expectations will raise the number of young people who emigrate to the developed lands. In the United States, pressure will grow to provide more, and less burdensome, economic assistance to qualified high school graduates who cannot afford to go on to college.

Pressure also will grow to make sure that all American students have access to an education capable of preparing them for college or a rewarding career.

Implications for Information Warfare and Operations: Young people concerned with economic success may be more vulnerable to blackmail or simple subversion. Beyond this distant possibility, no significant implications appear.

Expert Comments:

Ayers — There are, unfortunately, a number of nefarious cyber activities that young people seeking economic success (or those who feel they have been denied success) might be tempted to participate in. Employees can be paid by adversaries for acts of cyber-sabotage and identity theft, hackers can be hired for cyberterror, and unsuspecting kids could be paid to act as “cyber-mules,” carrying and delivering worms, viruses, and corrupted software as opposed to drugs. The simple act of negative

blogging about products and services, if directed by adversaries, could have severely negative impact on the economy. The Russian Business Network, a group of hackers operating from within Russia, could become a model for frustrated entrepreneurs in other countries. An additional concern is that those who feel they have not achieved the success they expected may be more likely succumb to online recruiting efforts by terrorist groups.

Pearson — We may have a whole generation of people deeply resentful that their expectations have not been met. Many young people in developed countries have been over-praised and are not ready for the global competition they will face.

Snyder — Everything I read about the "Millennials" reports that they are much more motivated by meaningful work than by economic success.

Sowa — As long as monetary gain remains THE primary indicator of valuation in the world, it will remain an easy component to get a mark to turn sides and act as an incentive for recruitment.

Tucker — According to a study at Florida State University, a growing number of U.S. teenagers harbor unrealistic expectations about what they can achieve. This generation-wide phenomenon could lead to anxiety, stress, and lost time and resources. This study tracked changes in high-school seniors, educational and occupational plans between 1976 and 2000 and found a significant and growing gap between stated goals and actual achievements. The research analyzed data from several national surveys, including the annual Monitoring the Future Survey, the National Longitudinal Study, the Digest of Education Statistics, and the Current Population Survey. Roughly 50 percent of high-school seniors in the year 2000 were planning to continue their education after college and get an advanced degree, and 63 percent planned to get a professional job such as doctor, lawyer, or college professor by age 30. In 1976, only 20 percent of seniors expressed similar goals. Meanwhile, the actual percentage of high-school graduates who obtained advanced degrees remained steady, suggesting that the gap between expectation and final outcome grew from 22 percent in 1976 to 41 percent in 2000.

16. Generation X, the Dot-Coms, and the Millennials are gaining social and organizational influence.

Members of each group—ranging from nearly 50 to the 20-somethings—have much more in common with their peers than with their parents. Their values and concerns are remarkably uniform throughout the world. Socially and in business, they are nearly color-blind and gender-blind. Generation X is starting new businesses at an unprecedented rate, and the Millennial generation is proving to be even more business-oriented, caring for little but the bottom line. They will work for others, but only on their own terms.

Generation X and the Millennials thrive on challenge, opportunity, and training—whatever will best prepare them for their next career move. Cash is just the beginning of what they expect. Employers will have to adjust their policies and practices to the values of these new and different generations, including finding new ways to motivate and reward them.

However, they also have a powerful commitment to society. Gen Xers are mainstays of "voluntourism," spending part of their vacations on volunteer work. In a recent survey, 60 percent of respondents said they would be interested in doing scientific or environmental work while on vacation. Even more would be willing to teach English or another academic subject.

Assessment: As trends go, this is an evergreen. In ten years or so, we will simply add the next new generation to the list.

Implications: In values, cultural norms, political issues, and many other ways, this change of generations will be every bit as transforming as the transition from the World War II generation to the Baby Boomers.

Employers will have to adjust virtually all of their policies and practices to the values of these new and different generations, including finding new ways to motivate and reward them. Generation X and the Millennials thrive on challenge, opportunity, and training—whatever will best prepare them for their next career move.

Cash is just the beginning of what they expect.

For these generations, lifelong learning is nothing new; it's just the way life is. Companies that can provide diverse, cutting-edge training will have a strong recruiting advantage over competitors that offer fewer opportunities to improve their skills and knowledge base.

Generations X and Millennial are well equipped for work in a high-tech world, but they have little interest in their employers' needs. They have a powerful urge to do things their own way. As both customers and employees, they will demand even more advanced telecommunications and Internet-based transactions.

Implications for Information Warfare and Operations: These generations are critical to the future of cyber-warfare and information operations. They supply both the cyber-savvy personnel capable of running information operations and the most directly info-dependent target group for disinformation and network disruption.

In general, "worldliness" makes people less drawn to "causes" and less apt to take action that might impede their success on their own terms. Unfortunately, this has proved not to be true in the Muslim world. The younger generations thus may also supply better educated, more sophisticated recruits to extremist and terrorist causes.

Probability is 50 percent; impact is medium.

Expert Comments:

Callanan — In addition to threats from developing countries, I believe that with the current and sudden economic downturn, the younger generation in more developed countries who have only known the good times are extremely vulnerable to the 'easy answers' that are often peddled by extremists. Many lack the means or adaptability to cope, unlike many of the older generation. This could result in a significant increase in disaffection amongst younger (and more technologically literate) people in more advanced economies.

Pearson — But they are competing with better motivated people in the developing world, so they may wield power, but in nations that are declining in importance.

Sowa — The three-generational groups mentioned here ARE critical to the future of cyber-warfare and information operations. BUT, it must be reminded that THESE GROUPS are primarily users … that is: they yield increasingly more complex demands for the use of the systems. However, the creators and actors within the system cannot be looked at solely by generational anecdotes (i.e. Arthur Clarke continued to bedazzle users right up to his death — as have all trend changers of this society).

Thus, it is essential to make use of Web 2.0 and Web 3.0, social networks, and other mainstream changes to monitor for emergent ideas — and what is ACTUALLY driving them. It is through this passive monitoring that we can better and more clearly grasp what is about to occur.

I have been using groups on Facebook, Blogs, Newsgroups, and other methods of social networking, for example, to obtain fresh scans on ideas for strategies and tactics for *Fortune* 1000 businesses. Much of the data mined is worthless, but occasionally, this approach draws more than just what one could obtain from Top-Down Focus Studies, or Futurist Scans.

Tucker — Members of the millennial cohort, according according to psychology professor Angela Provitera McGlynn, share a number of key characteristics that set them apart from their predecessors. In the United States, Millennials grew up in a time of largely uninterrupted economic prosperity; they're perhaps the most protected generation in history, in terms of government and safety regulations; and they are used to being indulged and consulted on family decisions. As a result, they tend to exhibit strong bonds with their parents. According to one survey, more than 75 percent of Millennials said they shared their parents' values.

Millennials are better connected both to their parents and to each other thanks to cell phones, text messaging devices, and e-mail. Some psychologists, according to McGlynn, see this bonding as positive, while others view it as an obstacle to the development of autonomy.

Millennials display an increased proficiency in multitasking, but are also known for attention problems and an inability to delay gratification. The Millennials, of course, were the first generation to grow up in the digital age. According to the 2005 Pew Internet & American Life Project, 2005, 87 percent of teens aged 12 to 17 used the Internet in 2004, up from 73 percent in 2000. In many ways, the World Wide Web (the largest component of the Internet) is itself Gen M.

Additionally, it is important to keep in mind that however spoiled they may seem, they won't be receiving many of the social or economic benefits their parents enjoyed such as stable pensions, a growing and stable economy, a healthy environment.

17. Two-income couples are becoming the norm in most of the industrialized lands, although in the U.S. the trend toward greater employment among women is slowing.

The percentage of working-age women who are employed or are actively looking for work has grown steadily throughout the industrialized world. In the United States, it has grown from 46 percent in 1970 to about 66 percent in 2005, compared with 77 percent of men. In Japan, a majority of households have included two earners since at least 1980.

In the United States, both the husband and the wife worked in 50.9 percent of married-couple families in 2003, according to the U.S. Bureau of Labor Statistics' Current Population Survey. This has declined since 1997, when it was 53.4 percent. However, families in which only the woman worked rose for the third straight year, to 6.8 percent, in 2003.

Assessment: In the industrialized nations, this trend has just about played out, as the number of two-income households has begun to stabilize. However, it will be a growing force in India and other industrializing lands for many years to come.

Implications: This emphasis on work is one big reason the richest 25 to 50 percent of the U.S. population has reached zero population growth. They have no time for children and little interest in having large families.

Demand for on-the-job child care, extended parental leave, and other family-oriented benefits can only grow. In the long run, this could erode the profitability of some American companies, unless it is matched by an equal growth in productivity. This also promotes self-employment and entrepreneurialism, as one family member's salary can tide them over while the other works to establish a new business.

Expect to see many families that usually have two incomes, but have frequent intervals in which one member takes a sabbatical or goes back to school to prepare for another career. As information technologies render former occupations obsolete, this will become the new norm.

Implications for Information Warfare and Operations: None are obvious.

Expert Comments:

Pearson — This just increases prices, since supply for many things is limited. Eventually, we are all working harder and harder just to stand still, causing frustration.

Sowa — The emphasis on work is driven by out-of-control consumption, and credit. This is a destabilizing factor on societies, as much as it creates economic sustainability. But, what it means is that desperate times call for desperate measures — desperate measures mean an increase in cyber-attacks. In societies where the culture does not treat women equally — women are seen more as the "mules" of society. As women become more professionalized and accepted in 20th Century male roles, and as they exceed their male counterparts in math and science, the statistical odds that increasing cyber-attacks will be managed by women will grow significantly.

ECONOMIC TRENDS

18. The economy of the developed world is growing steadily, with only brief interruptions.

When the United States catches a cold, the rest of the world gets pneumonia, or so economists used to say. Early in 2009, the United States has pneumonia. Home prices remain in free-fall, the credit market nearly frozen. In December, jobs were disappearing at a rate of more than 1 million every two weeks; a month later, the rate had slowed, but major corporations still were announcing job cuts daily. Consumer confidence is plummeting. Most of the world is in recession. It turns out that 2008 and at least some of 2009 are one of the interruptions contemplated in the trend.

Looking abroad, we can see effects of America's problems. The entire European Union is in recession. China, Australia, India, Japan, and Russia are in or near recession. In all, the economies of the world seem a lot less healthy than they did a few months ago.

Throughout the world, governments are scrambling to shore up lending institutions, stem the tide of foreclosures, restore the flow of credit, and provide jobs for the newly unemployed. These efforts will continue through 2009.

At that point, global economic growth will resume its accustomed rate, a bit more than 5 percent per year as of 2007.

Assessment: These trends have been revised many times since they were first codified in the late 1980s. Some trends have fallen off the list as they matured or as circumstances came along to change them. Others have been added as they were recognized. This trend has remained a constant, and with each revision its effective period has been extended. To invalidate this trend would take a catastrophe on the

order of the loss of Middle Eastern oil from the Western economies. No such dramatic reversal of global fortune can be foreseen.

Implications: New growth among all these trading partners should create a "benevolent cycle," in which the health of each partner helps to ensure the continued health of the rest at least through 2014. According to the World Bank, global growth is expected should come in at 2.5 percent in 2008, but only 0.9 percent in 2009, rebounding to 3 percent in 2010.

China has developed into an effective counterbalance for the U.S. economy. When America hits hard times, China can help to keep the world from following into recession. We first saw this in the post 9/11 crunch in the United States. This should make the global economy much more stable for so long as China remains a vibrant trading nation.

Any interruptions in economic growth should be relatively short-lived. By 2012 or so, India will expand faster than any other market in the world, with China falling into a close second place.

In the long run, the newly capitalist lands of the former Soviet Union should be among the fastest growing new markets, particularly if the oil industries of Kazakhstan and its neighbors, Kyrgyzstan and Uzbekistan, can be developed promptly. Labor markets will remain tight, particularly in skilled fields. This calls for new creativity in recruiting, benefits, and perks, especially profit sharing. This hypercompetitive business environment demands new emphasis on rewarding speed, creativity, and innovation within the workforce.

Implications for Information Warfare and Operations: One major reason the world economy has been growing so quickly and steadily is the continuing adoption of high technology to streamline business operations. Computers, automation, and high-tech communications such as the Internet all are increasingly critical to the functioning of industry, government, and even our personal lives. As other parts of this report make clear, we pay for these conveniences in vulnerability to disruption whenever something shuts them down. And in the future that could easily be a hostile nation or a non-state adversary skilled in information warfare.

Probability is 95 percent; impact is medium. As the world's economies become more clearly intertwined, their resilience against any specific attack improves. While a true systemic attack could start a downward spiral (such as that observed during the current recession), it will become harder to create such an event deliberately.

Expert Comments:

Pearson — This one may not be so brief, but we will get back on track. The next generation will be left with a lot of the bill, feeding intergenerational conflict. Countries are all trying hard to find the areas that they perceive as foundations of the future economy, so we will see large overshoot of investment in some areas, especially green

technology. The costs worldwide of going green to this extreme are probably far greater than the costs of the problems being addressed, and not everyone can win in the race to get the biggest share of the market.

Snyder — Not for the next 24 to 36 months, and perhaps longer!

The entire "economic trends" section contains no reference to the rising prosperity of developing nations, which the National Intelligence Council's November, 2008, *Global Trends 2025* report asserts will reduce the appeal of Islamic extremists. By failing to cite this trend, you also fail to draw attention to the fact that a prolonged global economic downturn will be likely to foster support for extremists.

Sowa — THIS NOTE IS CRITICAL: The current economic malaise follows the same fluid flow process akin to that of a network failing, a J-2 rocket engine, or an F-18 jet engine blowing out one of its sides, or that a power blackout. A single downed connection, or a power overload, or electrical spike, or an EMF wreaks havoc on the componentry of a single unit. To compensate, the power is automatically recircuited around the problem area or unit of the network. The energy involved doesn't go away, though. If it was an overload or surge, it will affect the recircuited areas of the grid, and they can also be damaged or even overloaded. This can cause system, process, material, or all-out failure.

In the integrated global economy, similar shocks to the system have system-wide repercussions. Only the extent of the damages varies from shock to shock. Cascading failures are often-cited and emergent phenomenon in any network. They are NOT independent, nor are they coincidental. Since the Great Depression, some partial protections to the global financial system have been in place. However, they have never been significantly tested or evaluated.

But, it has to be pointed out that any economic risks go much farther than just the financial. Because we have integrated many of our infrastructures—including cyberspace, and the electronic means to run our manufacturing and businesses—as well as the interconnectedness of our water supply, military materiel, energy and power transmission, oil and chemicals, biologicals, poverty, food, and even our ecosystems—we are now all impacted by any failures within these systems—and we should remain diligent on the ramifications of much more grave systemic threats and the global cooperation needed to implement a cooperative gridwork control system to avert the worst crises.

The ramifications of this to strategy and tactics in Cyberwarfare should be obvious. The potential systemic threats here are very probable at this juncture, and none of the mitigating solutions so far even take into account natural phenomena.

19. The global economy is growing more integrated.

By some counts, only half of the world's one hundred largest economies are nation-states. The rest are multinational corporations. In the European Union, relaxation of border and capital controls and the adoption of a common currency and uniform product standards continue to make it easier for companies to distribute products and support functions throughout the Continent. The Internet also brings manufacturers effectively closer to remote suppliers and customers. Companies are increasingly farming out high-cost, low-payoff secondary functions to suppliers, service firms, and consultants, many of them located in other countries. Companies in high-wage countries also are outsourcing management and service jobs to low-wage countries. An estimated 3.3 million U.S. jobs are expected to migrate to India and China by 2015. Some 40 million jobs are believed vulnerable to outsourcing.

Assessment: This trend will continue for at least the next two decades.

Implications: The growth of e-commerce enables businesses to shop globally for the cheapest raw materials and supplies. In niche markets, the Internet also makes it possible for small companies to compete with giants worldwide with relatively little investment. This has brought new opportunities for quality-control problems and fraudulent cost-cutting by suppliers, as seen in the recent spate of tainted food and other products coming from China.

The Net also has created a generation of "e-preneurs" whose businesses exist largely on the Internet, with production, fulfillment, and other functions all outsourced to specialty firms.

Demand will continue to grow for employee incentives suited to other cultures, aid to executives going overseas, and the many other aspects of doing business in foreign countries.

However, rising demand for foreign-language training is likely to be a temporary phenomenon, as more countries adopt English as part of their basic school curricula.

Western companies may have to accept that proprietary information will be shared not just with their immediate partners in Asian joint ventures, but also with other members of the partners' trading conglomerates. In high technology and aerospace, that may expose companies to extra scrutiny due to national-security concerns.

Establishing overseas branches mitigates this concern by keeping trade secrets within the company, even while gaining the benefits of cheaper foreign labor and other resources. Economic ties can give richer, more powerful countries considerable influence over their junior partners. Thus far, China has been the most successful at wielding this "soft" power. This has given it the ability to undermine American foreign policy even as it secures its energy and raw-materials needs.

Implications for Information Warfare and Operations: For "integrated," read "networked." The Internet, private networks, virtual private networks, and a host of other technologies

are quickly weaving the planet into a single, massively complex “infosphere.” These nearly infinite connections cannot be severed without overwhelming damage to companies, and even national economies. Yet, they represent unprecedented vulnerabilities to espionage and covert attack. This is another major trend for information warfare and operations.

Although the Internet was designed to work around damage, its complexity suggests that it conceivably might contain hidden vulnerabilities such that a single ill-trained user could inadvertently cause significant disruption.

See Trend 18 for probability and impact.

Expert Comments:

Forster — Greater economic integration increases interdependence and thus the ripple effect of disruption is far greater as is evident in the impact of the Russia-Ukraine gas dispute in January 2009. As a result, anything that disrupts the economy, such as a power outage caused by a hacked power system, will have a broader impact. Moreover, the convergence of economic disruption with trends such as expectation of economic success and two-income families increases the likelihood of civil unrest and potentially political instability. For example, it was not clear that Bulgarians would not take to the streets when faced with severely limited gas supplies.

Hoffman- Concur that interdependencies and even inadvertent linkages and networks are increasing vulnerability to cascading effects. Many of these networks are one step removed from effective security and expose numerous sites and individuals to unknown risks. Security and resilience systems are not keeping up.

Kapinos — Another thing to think about here: the sheer volume of information racing through the “info sphere” enhances the opportunity for cyber-war operators to embed encrypted information within routine data flows. This could take the form of system-disabling viruses, or secret message traffic concealed within an ocean of regularly-transmitted, legitimate data. Finding the bad data is the true search for the needle in a haystack. Sophisticated data-monitoring programs designed to detect unusual patterns would be needed to counteract such a scheme.

Pearson — This leads to more complexity of interactions, so it will be harder to spot points of vulnerability. Fraud and cyber terrorism will increase.

Peterson — This I believe is the ultimate Achilles heel—but it’s not limited to the economy. Physical networking integrates all global, national, and interpersonal C4I—government, military, commercial and social. How do you kill a hostile, self-replicating, avatar that takes residence in every device/multiple network buffers and attacks as part of the “call set-up” protocol in node to node contact?

Sowa — THIS IS A CRITICAL FOLLOW-ON TO MY NOTE FOR TREND 18: Corporations in the 21st Century are borderless and are NOT geopolitical. Ninety percent operate with a stated purpose to “maximize profits” for their stakeholders. In such an integrated global economy, shocks to the system, as I said in 18 have system-wide repercussions. Only the extent of the damages varies from shock to shock. Cascading failures are often-cited and emergent phenomenon in any network. They are NOT independent, nor are they coincidental. The key to actively thwarting Cyberwarfare is to recognize corporations and organized religions on the same—or even higher protocol—than geopolitical governments and borderless, non-geopolitical terror and extremist operations.

Cyberwarfare actors in these may or may not be acting with purposeful negative or criminal intentions. They may be acting for purposes to maximize profits for their stakeholders—who may not be of country-of-origin. But, in all cases they do represent unprecedented vulnerabilities to espionage and attack—AND AS SUCH ARE VERY LIKELY TARGETS TO ACT AS A “BASE” OR STAGING GROUND FOR FURTHER ESPIONAGE OR CYBER-ATTACKS.

Because of the interconnectedness, Corporations infiltrated by electronic, or by outsourced hiring practices can cause major mayhem and disaster to the networks of cyberspace. And, if not managed against, because we have integrated many of our infrastructures—including cyberspace, and the electronic means to run our manufacturing and businesses—as well as the interconnectedness of our water supply, military materiel, energy and power transmission, oil and chemicals, biologicals, poverty, food, and even our ecosystems—we are now all impacted by any failures within these systems—and we should remain diligent on the ramifications of much more grave systemic threats and the global cooperation needed to implement a cooperative gridwork control system to avert the worst crises.

The ramifications of this to strategy and tactics in Cyberwarfare should be obvious again. The potential systemic threats here are very highly probable as a threat at this juncture, and none of the mitigating solutions so far even take into account natural phenomena.

20. Consumerism is still growing.

Consumer advocacy agencies and organizations are proliferating, promoting improved content labels, warning notices, nutrition data, and the like on packaging, TV, the Internet, and even restaurant menus. On the Internet, shoppers themselves have access to a growing universe of information about pricing, services, delivery time, and customer satisfaction. Japan, China, and other markets are beginning the same revolution that has replaced America’s neighborhood stores with cost-cutting warehouse operations, discounters such as Wal-Mart, and “category killers” like Staples and Home Depot. As a result, consumer movements are springing up in countries where they have never existed. Consumer laws and regulations will follow.

Assessment: This trend seems likely to remain healthy for the at least the next 15 years.

Implications: Consumer advocacy agencies and organizations will continue to proliferate, promoting improved content labels, warning notices, nutrition data, and the like on packaging, TV, the Internet, and even restaurant menus.

Europe, Japan, China, and other markets are undergoing the same revolution that has replaced America's neighborhood stores with discounters.

However, the cultural and political power of farmers and small shop owners has slowed this trend in some areas, particularly in Japan.

Thanks to recent contamination of food imported from China, the U.S. Food and Drug Administration will be required to improve screening of incoming food products. However, it will not receive adequate funding to do the job effectively.

As prices fall to commodity levels and online stores can list virtually every product and brand in their industry without significant overhead, service is the only field left in which marketers on and off the Internet can compete effectively. Branded items with good reputations are even more important for developing repeat business.

Consumer debt may be an even greater problem for Millennials than it has been for their elders.

Implications for Information Warfare and Operations: Implications, if any, are obscure.

Expert Comments:

Pearson — [This trend could lead to] environmental instability if resources are not managed effectively, but actually, future tech should need less resource for a given quality of life, so consumerism can actually accelerate development towards more sustainability. Rapid obsolescence is key to making it work.

Sowa — Consumerism and advocacies are designed around market branding and identity development. Threats within these areas—as seen by the peanut butter problems of the FDA, and the campaign against government agencies as a result, will grow in cyberspace over the next 20 years—and will be a common resource for planting disinformation, or altering perceptions.

21. Research and development play a growing role in the world economy.

Total U.S. outlays on R&D have grown steadily in the past three decades. In 2006, the United States spent about $330 billion on R&D. China has taken second place in the world's R&D spending, with a budget estimate at $136 billion in 2006. China says it will raise its R&D spending from about 1.23 percent of GDP in 2004 to 2.5 percent in 2020.

R&D outlays in Japan have risen almost continuously, to nearly 3 percent of GDP, some $130 billion in 2006. R&D spending in the European Union (EU-15) amounted to $230 billion in 2006, about 1.9 percent of GDP. The European Commission has set a goal of raising R&D spending to 3 percent of GDP by 2010. In Russia, R&D funding is roughly 1.5 percent of GDP, up from just 0.7 percent in 1997; this amounted to about $26.25 billion in 2006. These figures do not include whatever clandestine military research escapes notice.

Assessment: This trend is stabilizing as developed nations, particularly the United States, devote more of their resources to less productive activities. We believe this is a temporary phenomenon. The trend will regain momentum in the years ahead. It will not fall off this list before the middle of this century.

Implications: This is a significant factor in the acceleration of technological change. The demand for scientists, engineers, and technicians will continue to grow, particularly in fields where research promises an immediate business payoff.

Low-wage countries such as China once took only low-wage jobs from advanced industrialized countries such as the United States. Today higher-paid jobs in science, technology, and the professions also are at risk.

Countries like India, China, and Russia once suffered a brain drain as those with high-tech skills emigrated to highdemand, high-wage destinations. Today, many students and professionals spend time in the West to learn cutting-edge skills, and then return to their native lands to work, start companies, and teach. This promotes the growth of some developing countries while reducing the competitive advantages of the developed world.

Implications for Information Warfare and Operations: Trend 21 is responsible for the accelerating technological advances seen in recent decades. It is another critical factor in the development of information warfare.

The chief product of R&D is not clever new merchandise or technologies, but information. Even the most sensitive output from research results are routinely stored in computers, shipped through company intranets, and usually transmitted over the Internet. This accessibility makes it a prime target for espionage, whether industrial or military. This problem has been growing nearly as quickly as the mass of information available to prying. It will be a still greater concern for security specialists in the years ahead.

Economic espionage will come to dominate the “black-hat” side of the cybersphere, displacing attacks motivated by the urge to cause damage for the sake of damaging. Witness the evolution of “hacking” and virus production, which are less often intended to damage the victim, but more to profit from the appropriation of information assets.

Probability is 95 percent; impact is high. Ongoing research has the greatest potential to shape the information environment.

Expert Comments:

Callanan — You might also wish to consider the emphasis that is placed within many R&D programmes on the dissemination of research results. While this is of course entirely sensible for the vast majority of research, the emphasis on getting as much information “out there” may pose additional security dilemmas in terms of cybercrime.

Olson — Spending on R&D for a growing company has to be about 10 to 15 percent of what is plowed back into the company, or the company dies. This has been true for at least the past 30 years. So this trend is not an increase unless you are talking about an R&D budget in excess of 15 percent, which I would find difficult to support, either as a company officer or as a future trend.

Pearson — Of course, the downside is that R&D also occurs in weapons tech, so there is always a background arms race. High capability technologies will present enormous threats to mankind in the second half of this century. I estimate average date of expected extinction as 2085. By accident or design.

Peterson — This isn’t true in real dollar terms. Incremental product engineering is now labeled R&D. The real innovation centers are obsolescent and substantive breakthroughs are fewer and farther between, and diffusion and assimilation rates are slower. Spin of packaged data not-with-standing; what is the market place telling us (university incubators, PARC, Bell Labs, etc.)?

Sowa — Research and Development—and especially the development of new technologies in every field—will continue to be the “great hope” that the world embraces to keep the economies and governments successfully operating. The value of R&D throughout history has been evident in all means of social, economic, political, and military success. Over the next 20-year cycle, R&D, and innovation from R&D, will accelerate exponentially in every country of the G20 — and beyond into the developing world.

In a more narrow range of cyberspace, new technologies will hold the keys to cyberwarfare, cyber-security, and cyber-attacks. This is a target-rich environment for espionage and attack. The actors to be defended against must include the traditional geopolitical organizations, but also the borderless, and non-geopolitical players mentioned prior, and the single lone- or small group actors.

22. Services are the fastest-growing sector of the global economy.

Service jobs have replaced many of the well-paid positions lost in manufacturing, transportation, and agriculture. Most of these new jobs, often part time, pay half the wages of manufacturing jobs. On the other hand, computer-related service jobs pay

much more than the minimum—for workers with sound education and training. Service industries provide 79 percent of the GDP in the United States, 77 percent in France, 74 percent in Britain, 73 percent in Japan, and 70 percent in Germany. In each case, services are growing rapidly, other sectors less so, and they provide substantial majorities of private non-farm employment. Production and less-skilled jobs, in contrast, are disappearing. By 2014, the United States is expected to have more chief executives than machine tool operators, more lawyers than farm workers.

Assessment: There is no foreseeable end to this trend.

Implications: In the United States, the growth of service industries is helping to deplete the middle class, as well-paid jobs in manufacturing are replaced by relatively ill-paid service positions, leaving a country of “have-a-lots” and many “have-nots,” but relatively few “have-enoughs.”

Services are now beginning to compete globally, just as manufacturing industries have done over the last 20 years. By creating competitive pressure on wages in the industrialized lands, this trend will help to keep inflation in check.

The growth of international business will act as a stabilizing force in world affairs, as most countries find that conflict is unacceptably hard on the bottom line.

Implications for Information Warfare and Operations: Some services, like dentistry and auto repair, deal with physical objects that must be near at hand. Many others deal primarily with information, sending more of it ricocheting around the world over the Internet each day. We already have commented sufficiently on the benefits and risks of networked information. Note only that this is one more factor contributing to their growth.

Probability is 100 percent; impact is low.

Expert Comments:

Pearson — The ‘physical economy’ can in principle be done by robotics, but much of the service economy could be done by smart robots, especially those with attractive AI personality. We may see this as a way to greatly increase standard of living, by adding large machine capability to the human economy.

Sowa — THIS NOTE IS CRITICAL: As services as a factor of all global economies grows—expertise in network infrastructures will grow with it. Manufacturing—even fully robotized and automated plants still operate at a slower pace than performing service transactions. The speed by which those transactions can occur is again a threat to maintaining control of the cyber-infrastructure, and as such control of just about every networked process and financial system worldwide.

23. Women's salaries are approaching equality with men's—but very slowly.

In the 1980s and '90s, women's overall income in the United States was catching up with that of their male co-workers. More recently, it has stagnated. In 1995, university educated women earned 75.7 cents for every dollar earned by men, on average.

In 2005, it had fallen to 74.7 cents. During the same period, lower-income women continued to gain on their male peers, though very slowly. One reason may be that women are less interested than men in working 70 hours or more per week during their prime reproductive years, and growing numbers have chosen to stay home and rear their children. Women also appear to be less likely to choose and pursue a career on the basis of income. Studies that attempt to compensate for differences in factors such as education, occupation, experience, and union membership find much smaller income differences than others. One reported that women receive about 91 percent as much as men. Another held that incomes are virtually equal when measured with appropriate rigor. Some studies also suggest that the pay gap has largely disappeared for women in the newest cohort of workers. This would make sense, given the nearly total gender blindness of the Millennials.

The same trend is visible in most other industrialized countries. According to the European Commission, women on the Continent earn 15 percent less than men, on average, down from 17 percent in 1995. In Britain, the gap was 20 percent, down from 26 percent. Japan is an exception to this trend. The gender gap there remains near 35 percent.

Assessment: In the United States, this trend may be in its last generation, thanks to the gender-blind values of the Millennials. In other countries, and particularly Japan, it may have another 30 years to run.

Implications: The fact that women's salaries are lagging despite higher academic achievement than men suggests that many college-educated women may be underemployed. Whether this is by their choice or occurs for some other reason has yet to be determined.

More new hires will be women, and they will expect both pay and opportunities equal to those of men.

Women's average income could exceed men's within a generation. College graduates enjoy a significant advantage in earnings over peers whose education ended with high school. In the United States, some 65 percent of young men and women enroll in college after high school, but women are more likely to graduate.

About 58 percent of college graduates are women.

To the extent that experience translates as prestige and corporate value, older women should find it easier to reach upper-management positions. This will blaze the trail and help raise the pay scale for women still climbing the corporate ladder.

Competition for top executive positions, once effectively limited to men, will intensify even as the corporate ladder loses many of its rungs.

The glass ceiling has been broken. One-fourth of upper executives today, and nearly 20 percent of corporate board members, are women—far more than in any previous generation. Look for more women to reach decision-making levels in government and business.

However, the remaining obstacles to women's advancement may explain why women now start businesses at roughly twice the rate of men.

Implications for Information Warfare and Operations: No significant implications have been identified.

Expert Comments:

Pearson — [Women's salaries are] taking a knock-back at the moment due to recession, but positive discrimination has in the past created some inefficient companies by putting people in positions because of their gender instead of their ability, and eventually the market decides who wins, not regulators. In some areas such as engineering, women earn more.

Sowa — Discussed earlier regarding its impact societally, and as a target for recruiting.

Tucker — Women around the world with access to the Internet will easily be able to garner first-hand information about how their circumstances differ from those of other women around the globe. Wild card: a mass women's migration away from the Muslim world as women seek brighter opportunities elsewhere.

WORK & LABOR FORCE TRENDS

24. Specialization continues to spread throughout industry and the professions.

For doctors, lawyers, engineers, and other professionals, the size of the body of knowledge required to excel in any one area precludes excellence across all areas. The same principle applies to artisans. Witness the rise of post-and-beam homebuilders, old-house restorers, automobile electronics technicians, and mechanics trained to work on only one brand of car. Modern information-based organizations increasingly depend on teams of task-focused specialists. For hundreds of tasks, corporations increasingly turn to consultants and contractors who specialize more and more narrowly as markets globalize and technologies differentiate.

Assessment: This process will continue for at least another 20 years.

Implications: In an information age, each new level of specialization provides greater efficiencies, reducing the cost of doing business even as it creates new opportunities. This should continue to make global business more productive and profitable for so long as it continues.

This trend creates endless new niche markets to be served by small businesses and individual consultants. It also brings more career choices, as old specialties quickly become obsolete, but new ones appear even more rapidly.

Implications for Information Warfare and Operations: Specialization implies a deeper knowledge of a narrower range of information and skills. Unfortunately, this largely precludes development of the generalized skills and grand-scale vision needed by top leaders in business, government, and the military. This may make it more difficult to find or train people to head organizations in complex, far-ranging fields, possibly including information warfare and operations.

It also is possible that some future threats may be overlooked because no one at the operating level has the breadth of understanding to notice the relationships between data or events in disparate specialties.

Probability is 95 percent; impact is high. Losing people with the ability to see global trends and tenuous relationships, with the vision to "connect the dots," will have impacts that resound for years.

Expert Comments:

Kapinos — I would just amplify what is already said here. As more specialization occurs, the value of "systems analysts" will increase. These are people who have the role of looking at, and analyzing the "big picture" — detecting and describing patterns and anomalies in broad, interconnected systems. Somebody has to be able to sit back and connect the dots — which wasn't done before 9/11, and may have been the critical breakdown in our early-warning system.

Pearson — It will increase until AI makes big inroads, in 2020s. Then people will quickly be relegated to interpersonal roles, with low levels of specialisation. This again creates vulnerability, since AI might displace people who understand how it works. If they are knocked out, no-one will know how to make the stuff work.

Sowa — Specialization is a problem—as we are losing people with the ability to see global trends and tenuous relationships—this problem will resonate for years.

25. The traditional age of retirement is losing its significance.

Organization for Economic Co-operation and Development (OECD) data show that people are retiring earlier in the developed world. In 2004, less than 60 percent of the 54 to 60 age group in the OECD countries had a job. This varied from 50 percent in the earliest-retiring nations to 76 percent in the latest. According to Pew Research, as of 2006 the average American worker planned to retire at age 61 but actually did so at 57.8. These “retirements” may not be permanent. Americans in particular often return to work and delay complete retirement for several years. About one in five people, and 40 percent of seniors, say they plan to continue working until they die.

Assessment: In the United States, this trend will be complete in a generation. Where social safety nets are stronger, it is likely to continue through at least 2030.

Implications: Given the widespread shortage of retirement savings and investments, most Americans will delay retirement until they can no longer work, whether they wish to or not.

Since the penalty on earnings of Social Security recipients has been rescinded, more American retirees will return to work, and those not yet retired will be more likely to remain on the job.

This trend will spread to other industrialized countries as the retirement-age population grows and the number of active workers to support them declines.

People increasingly will work at one career, “retire” for a while (perhaps to travel) when they can afford it, return to school, begin another career, and so on in endless variations.

True retirement, a permanent end to work, will be delayed until very late in life.

By 2015, we expect the average retirement age in the United States to be delayed well into the 70s. Benefits may also continue their decline, and they will be given based on need, rather than as an entitlement. Even though the Social Security program has been the “third rail” of American politics, within five years, the retirement age will be moved back at least to 70 for early retirement and full benefits at 72.

Retirees will act as technical aides to teachers, especially in the sciences. In the long run, it may prove impossible to maintain the tradition of retirement, except through personal savings and investment.

Implications for Information Warfare and Operations: For better or worse, this will keep the Baby Boom generation relatively influential long past the effective span of their forebears.

However, the direct impacts are ambiguous.

Expert Comments:

Pearson — Perhaps, but only for privileged elite, I think.

Sowa — Baby Boomers are the last generation to have been educated in liberal arts. Baby Boomers were the group that self-trained on the cyber technologies — learning far more of its roots "hands-on" and by solving real problems (not textbook), and understanding the ramifications and visions of its implementation. Baby Boomers created the global network and integrated themselves into its development.

Post-Baby Boomers have grown up using these global networks. They have a much deeper feeling that the network is a part of them—much as the automobile was a part of the post-War generation, and television and video was a part of the Baby Boomer generation. This feeling is emotive and represents an interesting and changing view of the global social culture.

The point is, that it should be essential for continuity and better processes to mine the wealth of data and information provided by Baby Boomers, as it will continue to have a major influence on the systemics of cyberspace. But, emergent trends and ideas need to grasp much more of the thoughts of Baby Boomers and post-Boomer generations.

Tucker — The fact that the Boomer generation is approaching the traditional retirement age has become regular fodder for the nightly news in the U.S. But the media tend to ignore the reality that Generation X and the Millennials should have no illusions about retiring at 65. In the years ahead, these two cohorts may begin to perceive this fact as evidence of social injustice.

The American private pension that the World War II generation enjoyed is now all but extinct. As companies like GM and American Airlines look for ways out of their current pension commitments, the last thing they are inclined to do is offer new pension agreements for recent grads. Today's workers will have to settle for a less lucrative, less stable 401Ks. As Jacob Hacker illustrates in his book *The Great Risk Shift*, the added risk of loss from a 401k vs. a pension is particularly stark, given the current recession.

Modern life is more expensive for young people today than it was when the Baby Boomers were just starting out. Economist Tamara Draut has estimated that the average debt for a college student in the U.S. is $19,000 in loans (up from $12,000 a decade ago.) The median consumer debt for 25- to 34-year olds is $12,000 or three times what it was twenty years ago, due in large part to deregulation in the credit industry. Meanwhile, the medium yearly income for a college grad has barely budged since 1974. The result: a college degree that's more expensive but doesn't pay more.

That debt comes on top having to pay for the public-sector portion of their parent's retirement. By 2030, there will be only three Americans of working age for every person over 65, compared with a ratio of five to one today. The only way to preserve today's entitlement benefits (Social Security and Medicare) will be either massive tax increases, massive deficits, or a government shut down in other areas. According to GAO comptroller general David M. Walker "Federal deficits will grow to unsustainable levels

in as little as two decades…At that point, without significant policy changes, federal deficits could reach 10 percent or more of our economy." In other words, Gen Xers and Millenials will be stuck with the bill for their Baby Boomer parents' partying ways.

Baby Boomers are also driving themselves bankrupt in record numbers. According to researchers John Golmant and Tom Ulrich, Baby Boomers are filing for bankruptcy at a much faster rate than the general population. Not surprisingly, the younger generations also are being told not to expect much by way of an inheritance. The median inheritance these days is anywhere from $30,000 to $50,000, a little less than the median income for a single year, and inheritances are in decline.

Gen X and the Millennials, who are the primary creators and consumers of online content and represent the future U.S. workforce, particularly the technical workforce, will feel more economically burdened than their parents.

26. Second and third careers are becoming common, as more people make mid-life changes in occupation.

Americans born at the tail end of the Baby Boom (1956 to 1964) held an average of ten jobs between ages 18 and 38, according to the U.S. Bureau of Labor Statistics. These job jumpers continue with short-duration jobs even as they approach middle age: 70 percent of the jobs they took between ages 33 and 39 ended within five years. In the United States, 23 percent of workers surveyed in 2004 reported being dissatisfied with their careers and considering a change of occupation. Seventy percent of Irish workers surveyed in 2004 also said they hoped to make a career change soon. Women and the 26-to-35 age group were most likely to report the desire to change careers. "Personal fulfillment" was the biggest reason cited for making the change.

Assessment: This trend will not disappear unless the pace of technological change slows dramatically—or we reach the so-called "singularity," when man's inventions grow so intelligent themselves that they entirely displace human beings from the workforce.

Implications: Boomers and their children will have not just two or three careers, but five or six, as dying industries are replaced by new opportunities.

"Earn while you learn" takes on new meaning: Most people will have to study for their next occupation, even as they pursue their current career.

In many two-earner couples, one member or the other will often take a sabbatical to prepare for a new career.

Self-employment is becoming an increasingly attractive option, as being your own boss makes it easier to set aside time for career development. This is especially true for Generation Xers and Millennials. Growing numbers of retirees will start their own businesses, both to keep occupied and to supplement their meager savings with new income. This trend has already begun. Retirement plans must be revised so that

workers can transfer medical and pension benefits from one career to the next—a change that has long been needed. We believe this will occur soon after the Baby Boom generation begins to retire in 2011.

Implications for Information Warfare and Operations: See Trend 25.

The need for multiple careers—potentially for several unrelated specializations in a single working life—may somewhat mitigate the problems noted in trend 25.

Thus, late-career workers may be a useful resource for the less technical aspects of information warfare and security, in which a broad understanding of potential targets, vulnerabilities, and their significance may be more important than hands-on experience with computer and communications equipment and software.

Probability is 95 percent; impact is medium. See comments at the end of Trend 25.

Expert Comments:

Pearson — Yes, people will change jobs more and more until they are no longer needed anywhere.

Sowa — Job-hopping provides almost a consultant's view of business operations. They may harness one-aspect of an operation (especially if it happens to be within their specialty) extremely well and deeply—but most often, unless operating at a C-level, will rarely understand any supplier or customer interconnectiveness. Job-hopping, like outsourcing, can be a beneficial trend or a nightmare in relation to aspects of cyberwarfare.

27. The work ethic is vanishing.

More than one-third of U.S. workers reported calling in sick when they were not ill at least once in the past 12 months, and 10 percent had done so at least three times, according to a 2004 survey by CareerBuilder.com. Job security and high pay are not the motivators they once were, because social mobility is high and people seek job fulfillment. Some 48 percent of those responding in a recent Louis Harris poll said they work because it "gives a feeling of real accomplishment." Fifty-five percent of the top executives interviewed in the poll say that erosion of the work ethic will have a major negative effect on corporate performance in the future.

Assessment: There is little prospect that this will change until the children of today's young adults grow up to rebel against their parents' values.

Implications: Both employers and voters must do their best to find candidates who can be trusted, but must expect to fail in their search. This makes safeguards against wrongdoing, both at work and in public lives, more important than ever.

The new generation of workers cannot simply be hired and ignored. They must be nurtured, paid well, and made to feel appreciated or they will quickly look for a friendlier, more rewarding workplace.

Training is crucial. Without the opportunity to learn new skills, young people will quickly find a job that can help them prepare for the rest of their many careers.

Implications for Information Warfare and Operations: High-mobility worker with little or no loyalty to their employers may represent a significant opportunity for the unauthorized transfer of information, whether to a new employer or to some external recipient. The profit motive could be significant here, particularly for workers who lost their previous job, rather than leaving it voluntarily.

Probability is 100 percent; impact is medium to low. While there will be more breaches due to mobility, each specific breach is likely be more limited and the impact less pervasive because short-term employees will be not entrusted with the most sensitive data.

Expert Comments:

Pearson — [This is true] only in developed countries, especially for young people who take it for granted that they will be rich and appreciated. They will get a shock as other countries come more and more on stream and take the markets away from them, leading to a releveling of the global playing field, along with salaries.

Sowa — High-mobility and low work ethics among workers, like job-hopping, and outsourcing prior, can be a beneficial trend or a nightmare in relation to aspects of cyberwarfare, the most common being mentioned breaches of security in the network, and high risks of targeting.

28. Labor unions are losing their power to secure rights for workers and to shape public policy in regard to workplace issues.

Union membership has been falling for the past two decades. In the United States, some 20 percent of workers were union members in 1983. In 2006, just 12.0 percent of employed wage and salary workers were union members, down from 12.5 percent a year earlier. In Britain, where the Thatcher government broke union power in the 1980s, union membership has declined almost continuously, to 28.4 percent in December 2006. In South Korea, where organized labor once was invincible, no more than 11 percent of workers are union members. One reason for this decline is that companies are freely seeking and finding nonunionized workers around the world. They also contract out a growing proportion of business activities to nonunion firms.

Assessment: In spite of determined, and occasionally successful, recruiting efforts in formerly non-union industries, union memberships and power will continue to decline for the next 15 years—until organized labor is little more than a fringe phenomenon. The

trend will be reversed only if Washington and other national governments rescind pro-business labor laws and policies enacted in the last 20-plus years.

Implications: For large companies, this trend promises continued stability in employee wages and benefits.

Unions eager to regain their membership will target any substantial industry or firm with less-skilled employees to organize. This could raise labor costs for companies that unions once would have considered too small to organize.

In ten to 15 years, American labor unions will compete with AARP to lead the battle for the rights of late-life workers and for secure retirement benefits. They face an inherent conflict between the interests of workers in what once would have been the retirement years and those of younger members, who rightly see the elderly as having saddled them with the cost of whatever benefits older generations enjoy. Unions' political strength is also diminishing and is increasingly being surpassed by powerful blocs such as AARP, Hispanics, and African Americans. The old paradigm of unions vs. corporations is obsolete. In today's economy, workers negotiate alongside management, winning shared bonuses.

Implications for Information Warfare and Operations: None are obvious, save perhaps that a worker with good pay, benefits, and job security under a union contract may be less vulnerable to temptations that could compromise his employer's data. However, this is more a general security issue than a specific implication for the current subject.

Expert Comments:

Pearson — Actually, they may well be replaced by cross-industry web-based bodies based on networking sites and their ability to act as platforms to mobilize power.

Snyder — This trend could reverse overnight in light of the widening disparity between managerial and rank-and-file incomes and pending pro-union legislation endorsed by Congressional Democrats and the President.

Sowa — Agree with said implications.

ENERGY TRENDS

29. Despite efforts to develop alternative sources of energy, oil consumption is still rising rapidly.

The world used only 57 million barrels of oil per day in 1973, when the first major price shock hit. By 2004, it was using 83 million barrels daily, according to the U.S. Energy Information Administration. Consumption is expected to reach 97 million barrels daily by 2015 and 118 million by 2030. Much of this increase will be due to China, which is the second-largest user of oil in the world, and the fastest growing.

Assessment: Nothing is likely to reverse this trend in the next 25 years.

Implications: Oil prices in much of 2008 were high enough to provide an incentive to develop new fields, such as the Arctic National Wildlife Refuge and the deep fields under the Gulf of Mexico. Environmentally sensitive areas will be developed using new drilling techniques, double-walled pipelines, and other precautions that make it possible to extract oil with less damage to the surroundings. Any future spike of oil prices to triple digits will erode support for environmental protections in the United States, leading to widespread development of whatever energy sources are most readily available, regardless of the long-term consequences to the environment.

Implications for Information Warfare and Operations: The growing role of automated controls to minimize energy costs opens new opportunities to disrupt important systems in manufacturing and transportation.

The price of oil also may encourage the replacement of travel with communications, bringing further opportunities for digital eavesdropping.

Probability is 45 percent; impact is low.

Expert Comments:

Forster — Continued reliance on a petroleum/gas-based economy increases the impact of cyberattacks on production and transportation systems. Disruption of GPS systems hamper transportation by supertankers, while the ability to compromise pumping stations and pipeline monitoring systems would negatively impact production and distribution. However, I disagree with this trend. The proliferation of technology and the oil shock of 2008, I believe, will hasten the development of alternative forms of energy. The impact will be to change the geopolitical balance, as the Middle East will become less critical to U.S. interests. This has the potential to further inflame Islamic extremism as undiversified economies in the region will suffer.

Pearson — There are very many new energy solutions being developed, far more than are needed to solve the problem, which is rapidly becoming just a short term problem. However, the intense focus on CO2 might be distracting from wider understanding of the environmental mechanisms, leading to vulnerability to other problems, such as effects of water vapour in the upper atmosphere, which could be just as bad a problem, but made worse by some of the CO2 solutions.

Sowa — THIS IS CRITICAL:

1. Oil will continue to dominate as the source of global energy for another 20 years.
2. Alternate energy will grow at a rapid rate over the next 20 years.
3. Energy transmission and fuel storage will dominate need over the next 20 years globally.

4. Energy transmission and fuel storage is a key technology transformation that must take place within cyber-network-systemics.
5. Replacing old infrastructure globally with “smart” infrastructure will be a key driver of economic growth over the next 20 years in all countries. This gives an edge to other countries who have no grids in place yet—but a massive retooling in the U.S., can be highly beneficial to our economy and future.
6. The building of the infrastructure, maintaining it, and maintaining security over it will be key to functioning in cyberwarfare and thwarting the potentials for dangerous “plants” in the system worldwide.

30. Contrary to popular belief, the world’s confirmed oil supply is growing, not declining.

As a result of intensive exploration, the world’s proven oil reserves climbed steadily since the 1980s and now hover at over 1.3 trillion barrels. Natural gas reserves stood at about 6.2 trillion cubic feet in 2007, about 1 percent more than a year earlier. Recent discoveries of major oil fields in Canada, Brazil, and under the Gulf of Mexico have substantially increased the world’s known oil reserves.

Assessment: Talk of “peak oil,” the suggestion that crude production has topped out, or soon will, is unjustified and, in FI’s view, unjustifiable. Our best estimate is that the world has used about one-fourth of its recoverable oil, and almost certainly no more than one-third. This trend will remain intact until at least 2040.

Implications: Higher oil prices should make it cost effective to develop new methods of recovering oil from old wells. Technologies already developed could add nearly 50 percent to the world’s recoverable oil supply.

OPEC will continue to supply most of the oil used by the developed world. According to the U.S. Department of Energy, OPEC oil production will grow to about 57 million barrels of oil per day by 2020.

Russia and Kazakhstan will be major suppliers if the necessary pipelines can be completed and political uncertainties do not block investment by Western oil companies. Russia will grow into the world’s second-largest oil producer by 2014; it would have been 2010, save for the global economic downturn that reduced oil demand, and price.

Alternative energy sources face problems with economic viability. Barring substantial incentives, this will inhibit efforts to stem global warming for the foreseeable future.

A generalized war in the Middle East after the United States leaves Iraq could drastically reduce the region’s oil output. This is unlikely, but the probable impact of such a conflict is so great that the possibility cannot be ignored.

The spread of fundamentalist Muslim regimes with a grudge against the West also could keep OPEC oil out of the American market. If the United States loses access to

Middle Eastern oil, it will buy even more from Canada and Venezuela, tap the Arctic National Wildlife Reserve, and develop the deepwater fields under the Gulf of Mexico much faster than expected.

In a prolonged energy emergency, America also would be likely to develop its vast reserves of oil shale, which have long been economically viable at crude prices over $40 per barrel. New technology reportedly makes it profitable at any price over $17 per barrel. With enough shale oil to supply its own needs for 300 years, the United States could become one of the world's largest petroleum exporters.

Developing shale would devastate the environment, but with crude oil prices in triple digits during a Middle-East war, the environment would be considered expendable.

Implications for Information Warfare and Operations: Like other new industries, shale oil production, alternative energy, and delivery systems will require substantial new data networks and automated controls. These will make interesting targets for the disruptive side of information warfare.

Probability is 45 percent; impact is low. While this trend will bring new vulnerabilities to be exploited by information warfare, the developed world offers so many other opportunities for attack that they will dwarf this trend's specific impact.

Expert Comments:

Pearson — Most oil will be left in the ground, as it will be much less in demand after solar power reaches cost parity and then continues to get cheaper. Sahara and other deserts will produce energy at $30 equivalent by 2030.

Sowa — Energy transmission will remain a critical component to maintaining cyber-systems. Cyber-attacks will key on attempting to "corner" this (on a geopolitical scale—i.e., Iraq's move on Kuwait, Russia's move into Georgia, etc.) or to "disrupt" this (i.e., partisan attacks in Southern Iraq near Basra, etc.). These attacks as the infrastructure becomes "smart" will most definitely be a highly-prized target of cyber-warfare.

31. When not perturbed by greater-than-normal political or economic instability, oil prices average around $65 per barrel.

New energy demand from the fast-growing economies of China and India has raised the floor that until 2004 supported oil in the $25 per barrel range.

Nonetheless, the spike in prices to nearly $150 per barrel in mid-2008 was an aberration. At least four factors contributed to the bubble in energy prices: Perhaps 30 percent of the increase in oil prices to their June 2008 high stemmed from the long-term decline in the value of the U.S. dollar on foreign exchange markets. Another $10 to $15 per barrel represented a "risk premium" due to fears of instability triggered by the Iraq war and Washington's threats to attack Iran. Without those two factors, $145 oil would

have been $100 oil. A worldwide shortage of refinery capacity helped to drive up the cost of gasoline, fuel oil, and other energy products. It appears that rampant futures speculation in the energy markets also helped to spur oil prices. None of these factors was permanent.

Assessment: Given the condition of the American dollar, it might be better to denominate oil prices in Euros—though this could be even more devastating for the American economy in the event of future episodes of instability. Aside from that, the long-term trend toward stable energy prices can only strengthen as the West reigns in consumption and alternative energy technologies become practical.

Implications: Barring an American invasion of Iran, oil prices of more than $100 per barrel cannot be sustained. New refineries in Saudi Arabia and other countries scheduled to come online by 2010 will ease the tight supply-demand balance for oil, and by then the Iraq war should be winding down. At that point, we can expect to see oil prices retreat gradually to around $65 per barrel. In response to high (by American standards) gas prices, the U.S. government probably will boost domestic oil production and refining to increase the reserve of gasoline and heating oil. This stockpile would be ready for immediate use in case of future price hikes. This will make it easier to negotiate with OPEC.

A key step in controlling oil prices, and an indicator of Washington's seriousness about doing so, would be development by the government of at least four new refineries around the country, probably for lease to commercial producers. To avoid problems with neighbors, the refineries could be located on former military bases, which the government already owns. We rate the odds at no more than 50:50.

In the long run, the United States almost certainly will drill for oil in the Arctic National Wildlife Reserve, though efforts will be made to minimize environmental damage. For example, drilling will take place only in the winter, when the tundra is rock hard. This small new supply of oil will have negligible effect on oil prices.

By 2020, the new fields under the Gulf of Mexico will come online, putting even more pressure on oil prices.

Implications for Information Warfare and Operations: There is at least a possibility that oil pipeline control systems and other aspects of today's energy infrastructure could become targets for cyber-war.

For probability, impact, and comments, see Trend 30.

Expert Comments: None received.

32. Growing competition from other energy sources also will help to limit the price of oil. Nuclear power is growing rapidly.

In Russia, plans call for construction of twenty-six more nuclear plants by 2030, when 25 percent or more of the nation's electricity will be nuclear. China plans to build thirty reactors by 2020, quadrupling its number and bringing nuclear energy consumption from 16 billion kWh in 2000 to 142 billion kWh. Even the United States is weighing the construction of new reactors.

For transportation, ethanol is the most useful alternative to petroleum. Brazil already gets more than 40 percent of its fuel for cars from ethanol made from sugar cane.

Renewable sources such as wind and solar power also are growing rapidly, but they are unlikely ever to make up more than a small fraction of the world's energy supply, save in areas where natural resources are plentiful. Iceland's drive to develop geothermal power is one example.

Assessment: This trend will remain in effect for at least 30 years.

Implications: Though oil will remain the world's most important energy resource for years to come, two or three decades forward it should be less of a choke point in the global economy. We should feed our stomachs before we feed our cars. Producing ethanol from switchgrass would cut the cost of corn by 20 percent, according to the Worldwatch Institute. This would significantly ease the global food crisis.

Solar, geothermal, wind, and wave energy will ease power problems where these resources are most readily available, though they will supply only a very small fraction of the world's energy in the foreseeable future.

Declining reliance on oil eventually could help to reduce air and water pollution, at least in the developed world. By 2060, a costly but pollution-free hydrogen economy may at last become practical.

Fusion power remains a distant hope. Cold fusion also remains a long shot for practical power, but FI believes it can no longer be discounted. If the U.S. Navy's reports of successfulexperiments can be corroborated, power plants based on the process could begin to come on line by 2030.

Implications for Information Warfare and Operations: Oil refineries, pipelines, and nuclear power stations are highly automated, high-priority targets for disruption in wartime.

For probability, impact, and comments, see Trend 30.

Expert Comments:

Pearson — Nuclear is becoming a red herring. It was a great solution but is starting to look expensive and too long term compared to developing efficient solar production. I no longer back it because of this, even though I used to be a big supporter.

Steele — As the developed world shifts to renewable and sustainable energy, the transitional period from dependence on oil consumption to new energy forms heightens the dependency on cyber-controlled systems. Connection to the global cyber network puts energy systems at risk. AI controlled solar collectors; wind, etc can be influenced by cyber and AI engagement.

TECHNOLOGY TRENDS

33. Technology increasingly dominates both the economy and society.

New technologies are surpassing the previous state of the art in all fields. Laptop computers and Internet-equipped cell phones provide 24/7 access to e-mail and Web sites. Flexible, general-service personal robots will appear in the home by 2015, expanding on the capabilities robotic vacuum cleaners and lawn mowers. New materials are bringing stronger, lighter structures that can monitor their own wear. By 2015, artificial intelligence (AI), data mining, and virtual reality will help most organizations to assimilate data and solve problems beyond the range of today's computers. The promise of nanotechnology is just beginning to emerge, but real possibilities range from high-powered super-batteries to cell-sized health monitors. Ultimately, speculations that we are approaching the "singularity's event horizon," the time when our artifacts become so intelligent that they can begin to design themselves and we cannot understand how they work, may prove correct. At that point, humanity will be largely a passenger in its own evolution as a technological species.

Assessment: Technologically related changes in society and business seen over the last 20 years are just the beginning of a trend that will accelerate at least through this century.

Implications: New technologies should continue to improve the efficiency of many industries, helping to keep costs under control.

However, this increased productivity has retarded United States job creation since at least 2002. Other developed countries are likely to feel the same effect in the future.

Technology made international outsourcing possible. It will continue to promote outsourcing to the benefit of the recipient countries, but to cause painful job losses in the donor lands.

New technologies often require a higher level of education and training to use them effectively. They also provide many new opportunities to create businesses and jobs.

Automation will continue to cut the cost of many services and products, making it possible to reduce prices while still improving profits. This will be critical to business survival as the Internet continues to push the price of many products to the commodity level.

New technology also will make it easier for industry to minimize and capture its effluent. This will be a crucial ability in the environmentally conscious future.

In 1999, a team at the technology organization Battelle compiled a list of the ten most strategic technological trends for the next 20 years. The list is available at the Battelle Web site. Key technologies for 2020, as forecast by Battelle:

• Gene-based medical care, from custom-tailored pharmaceuticals to cloned organs for transplantation;

• High-powered energy packages such as advanced batteries, cheap fuel cells, and micro-generators;

• "Green integrated technology" to eliminate manufacturing waste and make products completely recyclable;

• Omnipresent computing with computers built into consumer products, clothing, and even implanted under the skin;

• Nanomachines measured in atoms rather than millimeters that do everything from heating and cleaning our homes to curing cancer;

• Personalized public transportation that integrates our cars into a coordinated transport network, automatically picking the fastest routes and bypassing traffic jams;

• Designer foods and crops genetically engineered to resist disease and pests and be highly nutritious;

• Intelligent goods and appliances such as telephones with built-in directories and food packaging that tells your stove how to cook the contents;

• Worldwide inexpensive and safe water from advanced filtering, desalination, and perhaps even extraction from the air;

• Super senses that use implants to give us better hearing, long-distance vision, or the ability to see in the dark.

Implications for Information Warfare and Operations: This trend is the ultimate foundation for cyber-war. Complex, often delicate technologies make the world a richer, more efficient place. However, they also make it relatively fragile, as it becomes difficult to keep industries and support systems functioning when something disrupts computer controls and monitors, and the opportunities for disruption proliferate rapidly.

Some of these developments have very specific applications to information warfare and operations, either as new targets for data collection (nanotechnology, medical research,

aerospace, materials science, and energetics) or as opportunities for disruption (computers, networking.)

Probability is 95 percent; impact is medium. While the technological world will become more fragile and brittle, there is some reason to believe that specific systems will become more resilient and tolerant. A major re-dedication to infrastructure projects, as proposed in President Obama's economic stimulus program, may provide the impetus to continue to build fault-tolerant infrastructure that can, as the power grid is supposed to, self-correct and limit cascading impacts.

Expert Comments:

Coates –There seems to be a passion moving on to reality to robotize warfare. If it follows the airplane model, any useful number of them could break the bank. As information devices, how will they be fueled in the field? What happens when we retreat and leave them behind, or move out of country? The ubiquity of bright IT clever people has to be integrated into their use.

There is no discussion here of the use of IT by organized crime. I am frequently asked in my public lectures, what students should be studying, through college. One member of the audience said, "What about the Mafia?" One answer is obvious. "IT at MIT," It is 2015, and the Mafia electronically wipes out the records of a modest sized bank in Texas, or Nebraska or…. And then quietly visits a small group of large financial services organizations with a simple message: "We did it—you could be next. This is what we want, to protect you."

Forster — Obviously the ability to disrupt the technology infrastructure will have a greater impact on society.

Hoffman— I don't believe that "dominates" is correct. Technology is being exploited—"very unevenly"—by different societies and by different industries to lower costs, increase value, accelerate processes and delivery. Oddly, Bin Laden and his ilk are very effective at exploiting Western technology to promote a non-Western social system.

LaDuke — It was the dot.com bubble that brought the U.S. out of the last recession. The Web 3.0, deep Web, bubble is the best option to bring the U.S. out of this present recession. A global network of databases will be organized along a metadata spine (see www.ISEN.org) and semantic tools will tap into this significantly larger base of knowledge. These semantic tools will follow various models, e.g., mathematical representations of natural language structures that remove knowledge duplication.

This is an example of how the simultaneous convergence and rise of knowledge is coupled to the global economy and society. Adapting to technologies that naturally assist with this simultaneous convergence and rise of knowledge will create advantage. Resisting this flow creates recession or social disturbance.

Pearson — And ever more so in the future. It will become harder to police though, and more dangerous year on year. The benefits will be huge, but so will the risks. There are just too many nutters out there.

I think local government and civil service departments make ideal targets, since they are not so well protected as national government, but can cause just as much disruption if attacked.

Rowlatt — It is very difficult to predict the future of technology for two reasons more than anything else; firstly it is driven by consumer demand (this regulates business R&D funding), secondly it is also influenced by business' R&D secrecy and roll out plans.

Big business does not want to share its future development ideas, as this is all about industrial espionage. They will conceive an idea then stuff it under the table until the market is right for them to turn a profit, or shape the market for a future technology that will give them greater leverage.

The challenge then is not trying to predict technology, but being able to more accurately assess its impact on society or utility as a weapon.

We need to be able to predict the development potential of technology as it emerges. Even a company that releases a product, may not truly understand the product's potential if they have not seeded enough funding into the initial R&D process.

Sowa — Technology will alter all the current traditional thinking about cyberspace, cyber-warfare, and traditional warfare. Because it will be totally interlinked to the network its ramifications will be costly, and widespread. Battelle Institute, the NSA, the Materials Research Society, NASA, the military branches, and numerous other entities have made significant trend projections in this area. WHAT MUST BE EXPLORED is how, for example, cellular or water-based computing systems, artificial intelligence, and things like singularity will have specific impacts on cyber programs currently existing, in R&D, in production, or being funded. For example, SEAL Team stealth craft and Navy Destroyers being worked on by Converteam will only remain stealthy as long as the internal wiring and routing system and switches run on fiber—not copper. Yet, current DoD supply vendors do not offer such essential componetry. To handle all aspects of cyberwarfare correctly, these kinds of mindless systemic snafus require adequate futurecasting and analysis. Otherwise, many of our systems will become outdated before they are even production-ready. And, these will greatly add to the total cost of the program—even if short-term budgetary costs are reduced.

Steele — A challenge to information security is an anachronism in Singularity engagement scenario. Cyber systems are cyber realities. Much more holistic in nature—not simply information but cyber cultures.

Coordinated Cyber attacks at multiple levels will be capable of knocking out macro (national defense systems), meso (local power grids), and micro (starting an automobile) simultaneously.

Thomas — Impact of cyber attack characteristics (anonymity and plausible deniability) on policy and responses: nations have to hold back responses because they can't be sure just who is reconnoitering their systems.

Inability to understand impact of culture on methods that nations use the Internet: For example, the Chinese use electrons as carriers of strategies, a concept the US has never followed to the best of my knowledge

34. The United States is ceding its scientific and technical leadership to other countries.

"The scientific and technical building blocks of our economic leadership are eroding at a time when many other nations are gathering strength," the National Academy of Sciences warns. "Although many people assume that the United States will always be a world leader in science and technology, this may not continue to be the case inasmuch as great minds and ideas exist throughout the world. We fear the abruptness with which a lead in science and technology can be lost—and the difficulty of recovering a lead once lost, if indeed it can be regained at all."

Although R&D spending is growing in raw-dollar terms, when measured as a percentage of the total federal budget or as a fraction of the U.S. GDP, research funding has been shrinking for some 15 years. In 2005, the United States spent about 2.68 percent of its GDP on R&D, down from 2.76 percent in 2001. Washington has often reduced the post-inflation buying power of its R&D funding request. In the FY 2007 budget, for the first time, it cut R&D funds in absolute dollars as well. Washington's neglect of basic science is being felt in many ways. Only half of American patents are granted to Americans, a number that has been declining for decades. Only 29 percent of the research papers published in the prestigious Physical Review in 2003 were by American authors, down from 61 percent in 1983.

More than half of American scientists and engineers are nearing retirement. At the rate American students are entering these fields, the retirees cannot be replaced except by recruiting foreign scientists. Between 25 percent and 30 percent of high school graduates who enter college plan to major in science or engineering. Fewer than half of them receive a degree in those fields. The number of U.S. bachelor's degrees awarded in engineering in 2005 was nearly 15 percent below the peak 20 years earlier

Assessment: This trend emerged from a wide variety of ill-conceived political decisions made over the last 30 years. It will take at least a generation to reverse.

Implications: If this trend is not reversed, it will begin to undermine the U.S. economy and shift both economic and political power to other lands. According to some

estimates, about half of the improvement in the American standard of living is directly attributable to research and development carried out by scientists and engineers.

The Bureau of Labor Statistics predicts that the number of job openings in science and engineering will grow by 47 percent in the five years ending 2010—three times as fast as nontechnical fields. The United States will not produce nearly enough home-grown technical specialists to fill them. Demand to import foreign scientists and engineers on H-1B visas also will continue to grow.

Publicity about the H2-B program, and about the offshoring of R&D to company divisions and consulting labs in Asia, in turn, will discourage American students from entering technical fields. This has already been blamed for shrinking student rolls in computer science.

In 2005, China for the first time exported more IT and communications goods ($180 million) than the United States ($145 million.) Its lead has grown each year since then.

Implications for Information Warfare and Operations: To whatever extent the United States loses its leadership in science and technology, it falls behind other countries in the intellectual and personnel base required for information warfare and operations. If this trend is not reversed, the U.S. could find itself at a significant disadvantage in this strategically and tactically important area.

In the specific fields of computers and networking, the greatest threats may come from Russia and the other states of the former Soviet Union, rather than from China or India. Russia and Bulgaria in particular have had strong programs in computers and networking, and Bulgaria has long been a global capital of computer virus and network development. The infrastructure of personnel required to implement new information warfare programs or to continue existing ones has largely survived the years since 1989.

Probability is 50 percent; impact is high. Without the brain, the body becomes vulnerable. Without a strong base of highly educated workers, the United States simply will not be able to compete in the world marketplace. Probability is reduced because we anticipate a resurgence in American education.

Expert Comments:

Anonymous — I find that the number of person's entering a field is not the important metric. The quality of those people is the critical measure.

Coates — I think that half of your first sentence is unsustainable, that our scientific and technological building blocks are eroding. There is confusion between other countries doing better, implying that we are doing worse. It can only be good for humankind if we have numerous centers of excellence rather than follow some football game model, that you are on top or you are nothing. Again you repeat the point, or more properly the

allegation, that our technological capabilities are deteriorating. I must see an article every two weeks claiming that—and offering no support.

Hoffman — A bit alarmist in tone, we had an artificial lead in some respects due to the second World War and even the Cold War. Yes, this advantage is slipping over time, but as Zakaria and Berkowitz have written in their books we retain a lot of systemic advantages. The world is returning to a normal distribution of power, and we retain advantages in size, allocation of capital, rewards and incentives and education. Overall, our position is diminished and we need to be conscious of how we can best preserve a competitive advantage.

LaDuke — The strength of the U.S. is in knowledge creation under the auspices of innovation and invention that has been applied in all kinds of technologies. Ceding existing technology as technology converges and rises exponentially is not as significant as not creating the knowledge that is empowering future advances in technology. Any looking backward at threats is at the least distracting and at the most counterproductive.

Pearson — The increased power of smart individuals is more of a problem, espcially in NBIC areas. Unabomber style activity from inconspicuous people within a community is more of a danger than hostile states or terrorist groups.

Sowa — The impact and fallout of losing scientific, technical, and engineering leadership is a high-risk trend. The US will lose its standing in all areas—militarily, economically, and socially. This threat is far-reaching. Russia and Bulgaria are mentioned as high threats—but the list should actually include much of Eastern Europe, and former satellites of the USSR, as well as our “neighbors” in North, Central, and South America, Micronesia, Indonesia, and the Caribbean.

Steele — Not only is the U.S. ceding the “left brain” sciences, but the continuation of a linear, industrial model for education has the U.S. ceding a growing need for “right brain”—creative and synergistic thinking. Humans (and transhumans, androids on one hand and genetically altered humans on the other) living in the “Singularity Engagement” era will need thinking with left and right brains and synthesize direct information upload to the human brain.

Failure to adopt 21st Century thinking. Systemic failure to rapidly create processes for combating and thinking about nonparadigmic states of being produces vulnerability. Searching for questions with multiple answers (vs. paradigmic searching for “the right answer…”) becomes a way to engage cyber war in the current and future century. Intense training in this “way of thought” that is beyond creative problem solving but rather creative reality creation enhances societal capability and human capacity.

35. Important medical advances will continue to appear almost daily.

Research into human genetics, stem cells, computer-aided drug design, tissue transplants, cloning, and even nanotechnology promise to ease or cure diseases and injuries that do not respond to today's medicine. Radical new treatments for diabetes, Parkinson's disease, perhaps Alzheimer's, and many other disorders are expected to arrive within the next five to ten years. Scientists even are beginning to understand the fundamental processes of aging, bringing the possibility of averting the diseases of old age, and perhaps aging itself.

Assessment: The flow of new medical advances will not slow in the next 40 years, and probably not in the next 75.

Implications: In the next ten years, we expect to see more and better bionic limbs, hearts, and other organs; drugs that prevent disease rather than merely treating symptoms; and body monitors that warn of impending trouble. These all will reduce hospital stays.

Outside the United States, transplants of brain cells, nerve tissue, and stem cells to aid victims of retardation, head trauma, and other neurological disorders will enter clinical use by 2012.

Laboratory-grown bone, muscle, and blood cells also will be employed in transplants.

Expect also the first broadly effective treatments for viral diseases, experimental regeneration of lost or damaged human tissues, and effective ways to prevent and correct obesity.

By 2025, the first nanotechnology-based medical therapies should reach clinical use. Microscopic machines will monitor our internal processes, remove cholesterol plaques from artery walls, and destroy cancer cells before they have a chance to form a tumor.

Forecasting International believes that cloning and related methods will be accepted for the treatment of disease, though not to produce identical human beings.

Even without dramatic advances in life extension, Baby Boomers are likely to live much longer, and in better health, than anyone now expects. However, this trend could be sidetracked by the current epidemic of obesity, which threatens to raise rates of hypertension, diabetes, heart disease, and arthritis among Boomers if a cure is not found quickly enough.

However, a significant extension of healthy, vigorous life—to around 115 or 120 years as a first step—now seems more likely than no extension at all. The most significant question remaining, other than the scientific details, is whether it will arrive in time for the Baby Boom generation to benefit or will be limited to their children and descendents.

High development and production costs for designer pharmaceuticals, computerized monitors, and artificial organs will continue to push up the cost of health care far more

rapidly than the general inflation rate. Much of these expenses will be passed on to Medicare and other third-party payers. Severe personnel shortages can be expected in high-tech medical specialties, in addition to the continuing deficit of nurses.

Removal of barriers to stem-cell research in the United States could speed progress in this critical field. This could be expected to produce new treatments for neurological disorders such as Parkinson's and Alzheimer's disease and many other illnesses now incurable or untreatable. It also would recover one aspect of America's lost lead in science.

Implications for Information Warfare and Operations: This trend is responsible for the growing number of older, fitter seniors who are likely to remain active and influential, and suitable targets for information operations, well into old age.

Growing computerization and networking of medicine in the United States and Europe could open new vulnerabilities to cyber-warfare. (Imagine, for example, being able to delete references to a drug allergy from a national leader's medical records and insert a prescription for that medication!) Potential target countries for American operations are likely to be much slower in developing this kind of exposure to disruption.

Medical research is relatively unlikely to be classified, though much of it may remain unpublished until the resulting technologies can be patented. However, nanotechnologies developed for medical purposes could well have applications that require classification. In the future, such information could be a prime target for computerized espionage.

Probability is 50 percent; impact is low. Given the current state of American health care, information based attacks may have a high impact in a specific single incident, but medical errors attributable to human mistakes will continue to overshadow any intentional attack vector. This may change if the Obama administration's effort to computerize the health care industry for efficiency comes to fruition.

Expert Comments:

LaDuke — Viral or nano replication is the most threatening technology on the horizon. But because these are indiscriminate, they will not likely be purposefully or rationally employed. However, this technology will evolve to become genetically selective, sensing and attacking a specific genetic code—effectively creating a race extinction machine.

Pearson — Costs of better care via high tech will not inevitably increase for ever, there may well be an inflection point where advanced technology starts to improve health so well and so cheaply that overall health costs start to fall sharply.

Sowa — Advances in biotechnology will allow for machine-human melding over the next 20 years, bionic implants, and other interjected components in humans make them cyber-mules to transport in and out all kinds of cyber-capable data.

Tucker — Nanomedicine could have a wireless component, and that signal could conceivably be hacked. Consider: In 2006, Welsh cyberneticist Kevin Warwick had an experimental Internet-ready microchip surgically implanted in his head. Building off the success of widely available implants like cochlears, which treat certain types of deafness, Warwick's implant research dealt with enhancing human abilities. In a December 2006 interview with IT Wales, he discussed an experiment he took part in with his wife wherein they actually traded neural signals—a crude form of telepathy.

"We had my implant which linked my nervous system electrically directly with the computer and onto the Internet, and my wife Irina, who also had electrodes pushed into her nervous system to link her nervous system to the computer and the Internet, and we essentially linked our nervous systems together directly, electrically. So that when she moved her hand, the neural signals from her brain went from her nervous system and appeared on my nervous system, and therefore up to my brain. So her brain signals traveled electrically to stimulate my nervous system and brain, and when she moved her hand three times, I felt in my brain three pulses, and my brain recognized that my wife was communicating with me. It was the world's first purely electronic communication from brain to brain, and therefore the basis for thought communication."

Further experimentation will likely proceed along these lines.

36. Transportation technology and practice are improving rapidly.

The newest generation of aircraft, such as the Boeing 787 and future Airbus A350 XWB, are using lightweight materials and more efficient engines to cut fuel costs, stretch ranges, and increase cargo capacity. In the United States, two companies have even announced plans to build supersonic business jets and have them in the air by 2013 or so. One has already taken deposits for several dozen aircraft. At the same time, rail travel is getting faster. The new TGV Est line, which runs 300 km (180 miles) from Paris to Frankfurt, operates at 320 kph (198.8 mph) inside France, compared with 300 kph on other parts of the TGV system. China has begun to install a network of high-speed trains to compensate for its shortage of regional air transportation.

Assessment: These advances will continue at least through mid-century.

Implications: One of the fastest-growing transport industries is trucking, thanks to the expanded use of just-in-time inventory management and Internet-based companies that rely on trucks to deliver their products. This field will grow more efficient as GPS-based truck tracking, RFID-based cargo management, more efficient engines, and other new technologies spread through the industry.

To reduce the number and severity of traffic accidents, trucks on the most heavily used highways will be exiled to car-free lanes, and the separation will be enforced.

New hybrid car models will begin to gain significant market share from traditional gas guzzlers between 2010 and 2015.

By 2010, smart-car technologies will begin to reduce deaths due to auto accidents in Europe and, a few years later, the United States.

Cities increasingly will struggle to reduce auto congestion by limiting the use of private automobiles, as in Munich, Vienna, and Mexico City; by taxing auto use in congested areas, as in London; or by encouraging the development and use of mass transit, as in Copenhagen and Curitiba, Brazil.

Technology may offer other alternatives. One proposal is “dual-mode transportation,” in which private cars would be used normally on short hauls but would run on automated guideways for long-distance travel.

Implications for Information Warfare and Operations: Growing reliance on GPS navigation, in-car communications, automated rail systems, and other transportation technologies creates more opportunities for disruption.

Probability is 55 percent; impact is medium. While this trend will create new vulnerabilities to information warfare, they will be just a few among many, partially mitigating this trend’s specific impact.

Expert Comments:

Pearson — More use of automated systems and networking gives an increased range of channels and targets.

Sowa — The largest changes in the next 20 years that will impact transportation AND cyberwarfare will come from advances in material science. The new lightweight materials mentioned make non-metallic UAV systems possible, and fuel storage for longer flights probable—a poor man’s cruise missile driven by GPS to targets within the range of the new fuel storage elements. These combined with traditional ICBM-capable rocketry driven by more exacting telemetry from commercial providers—basically change the culture of cyberwarfare from stationary networks to mobile and wireless operations.

37. The pace of technological change accelerates with each new generation of discoveries and applications.

In fast-moving engineering disciplines, half of the cutting-edge knowledge learned by college students in their freshman year is obsolete by the time they graduate. The design and marketing cycle—idea, invention, innovation, imitation—is shrinking steadily.

As late as the 1940s, the product cycle stretched to 30 or 40 years. Today, it seldom lasts 30 or 40 weeks. Almost any new consumer product can be exactly duplicated by Chinese factories and sold on e-Bay within a week after it is introduced. The reason is simple: Some 80 percent of the scientists, engineers, technicians, and physicians who ever lived are alive today—and exchanging ideas real time on the Internet.

Assessment: This trend will continue for many years. However, we may grow less able to perceive it.

Implications: Subjectively, change soon will move so rapidly that we can no longer recognize its acceleration, save as an abstract concept.

All the technical knowledge we work with today will represent only 1 percent of the knowledge that will be available in 2050. Industries will face much tighter competition based on new technologies. Those who adopt state-of-the-art methods first will prosper. Those who ignore them will eventually fail.

Products must capture their market quickly, before the competition can copy them. Brand names associated with quality are becoming even more important in this highly competitive environment.

Lifelong learning is a necessity for anyone who works in a technical field—and for growing numbers who do not. In what passes for the long run—a generation or two—the development of true artificial intelligence is likely to reduce human beings to managers. Rather than making new discoveries and creating new products, we will struggle to understand and guide the flow of novelties delivered by creations we cannot really keep up with.

Implications for Information Warfare and Operations: As new technologies arrive, industry will be forced to hire more technology specialists and to train other employees to cope with new demands. Some support functions may be moved offshore, where technically knowledgeable adversaries might have greater access to them, opening the way to disruption.

Some of the most interesting possibilities may emerge from the spread of RFID (radio-frequency identification) chips throughout industry. Among other benefits, RFID makes it easier to implement just-in-time sourcing of manufacturing components, retail and wholesale stocks, military supplies. This offers operational and financial efficiencies, but squeezes useful padding out of the system. Any disruption of RFID-based inventory, ordering, and transportation systems could result in significant shortages at the end-user level. In the civilian economy, this would cause economic hardship. In the military world, consequences could be more severe.

Probability is 55 percent; impact is medium.

Expert Comments:

Coates — It is important in the discussion not to neglect the large amount of information technology now obsolescent or obsolete, but in place. We did a small and unclassified study of that subject for the NSA a few years ago.

Forster — Proliferation of technology facilitates the coalescence of unrelated but networked organizations (criminal and terrorist) in the execution of an operation.

Hoffman — Yes the potential for greater convergence of various technologies will accelerate the development and introduction of new systems and techniques. This will require constant adaptation by systems managers and constant learning at the individual level. Whatever you were taught in undergraduate school is certainly going to be obsolescent before you take a graduate degree. Does our educational system support this? Do government personnel systems recognize this?

LaDuke — Accelerating change is accelerating knowledge advance and subsequent application of that knowledge. Knowledge advance is the sum of knowledge creation. As such, knowledge creation is central to accelerating change.

There is a strong distinction between cyber attacks like information security breaches, virus/worm intrusions, or denial/disruption of service attacks and the 'cyber arms race' of social advance and subsequent application that can shift the balance of power. Social advance is the ultimate cyber weapon because it results in advances in information security, intelligence gathering, physical weapon systems, all kinds of technologies, economies, etc. Advantage in accelerating change is in knowledge creation and the key to knowledge creation is in understanding the question.

There are two primary types of questions, 1) learning questions, which are questions about knowledge that exists and 2) knowledge creation questions, which are questions answered to create knowledge that does not yet exist. The nano, bio, info, cognitive science or NBIC convergence is in fact a progression toward an understanding of these question types. As we advance toward singularity, knowledge will continue to converge and we will understand that we've over complicated three core technologies. The one will rely on a rational method akin to scientific method to eliminate all duplication and automatically taxonomize knowledge into one. The second will allow smart search and retrieval of this one knowledge (that exists.) The third will be artificial knowledge creation, which will automatically create new knowledge, by logically extending existing context.

Knowledge creation is a repeatable process that is performed by humans and could be performed by machines exclusively or in systems built to interact with humans ("Man-in the-loop" systems.) Artificial knowledge creation (AKC) will usher in singularity, not artificial intelligence (AI) or artificial general intelligence (AGI) or technology advancing itself. Artificial intelligence (AI) has already been achieved by any computer because intelligence is appropriately defined as knowledge stored that can be retrieved (by human or computer.)

The first arriver to this technology will drive the entire paradigm shift.

Pearson — The singularity is a real risk, when new weapons or analysis of existing systems to find security holes becomes too rapid.

Sowa — This trend has a “high” impact and probability.

Steele — Uploading cyber information directly to humans and to AI systems, then instantaneously morphing this information in creative alternatives produces a virtual and instantaneous change environment. This will require cyber system (beyond human) thinking and symbiotic cyber-human relationships (as well as cyber-cyber relationships.)

A Scenario Builder -Toward a model of cyber combatants, 2035. While there are many variables that influence cyber war, this model reflects the intersection of lethality, visibility and frequency. It is offered for reflection and further development if relevant. It is a typology. Probabilities would need to be assigned.

Examples:

The first two elements (Human-human and Technology/Cyber Enhanced) are familiar as they reflect human evolution on the planet to this point. The elements suggest everything from hand-to-hand combat to smart and intelligent weapons used by humans on humans. This is the current state as increasingly smart weapons engage humans (simple example, drones) and cyber system on cyber system launched by humans.

Singularity engagement suggests cyber systems creating AI and technological weapons and using them independent of or engaged with humans.

38. The Internet continues to grow, but at a slower pace.

In mid-2007, Internet users numbered about 1.173 billion, up just less than one-fourth in three years. Most growth of the Internet population is now taking place outside the United States, which is home to only 19 percent of Internet users. In mid-2007, the most recent available data showed 162 million Internet users in China (12.3 percent of the population), 42 million in India (3.7 percent), and 86.3 million in Japan (67.1 percent.)

The growth of e-commerce also is slowing, with 2007 sales coming in at $116 billion Sales growth, as much as 25 percent per year in 2004, is expected to slow to 9 percent annually by 2010. The current recession may trim up to 2 percent off that pre-2009 forecast, but growth will continue at its expected pace thereafter.

Assessment: Internet growth will continue until essentially no one in the world lacks easy access to e-mail and the Web, about 30 years by our best estimate.

Implications: Americans will continue to dominate the Internet so long as they produce a substantial majority of Web pages—but that is not likely to be very long.

Analysts believe that Internet growth will not accelerate again until broadband service becomes less expensive and more widely available. This is a matter of government policy as much as of technology or basic costs.

Demands that the United States relinquish control of the Internet to an international body can only gain broader support and grow more emphatic as Americans make up a smaller part of the Internet population.

B2B sales on the Internet are dramatically reducing business expenses throughout the Internet-connected world, while giving suppliers access to customers they could never have reached by traditional means.

The Internet has made it much easier and cheaper to set up a profitable business. An online marketing site can be set up with just a few minutes' work at a cost of much less than $100. This is fostering a new generation of entrepreneurs.

Internet-based outsourcing to other countries has only just begun. Growth in this field will accelerate again as overseas service firms polish their English, French, and German and find even more business functions they can take on.

Cultural, political, and social isolation has become almost impossible for countries interested in economic development. Even China's attempts to filter the Internet and shield its population from outside influences have been undermined by hackers elsewhere, who provide ways to penetrate the barriers.

Implications for Information Warfare and Operations: The slowing of the Internet is relatively insignificant, especially when you consider how rapid its expansion has been to date. The Net already has become the primary medium for and target of information warfare.

As the Internet further penetrates the Muslim lands, it may open new opportunities for attacks on the West, particularly in the economic realm. In the relatively short term—say, a generation or two—growing exposure to relatively uncensored Western thought is likely to provoke a strong backlash in conservative parts of the Muslim world. Yet, over time it may ease the relationship between this disparate cultures.

Countries that, like China, attempt to block their citizens from open access to the Net may have an advantage in information warfare and operations. The so-called "Great Firewall of China" represents an opportunity to train large numbers of personnel in network operations and security, and in methods of defeating network security systems.

Probability is 85 percent; impact is low. Many of the potential modes of attack on the Internet already are well known, and the pace of growth on its own will not change them or create new ones.

Expert Comments:

Pearson — I don't agree. It still hasn't reached anything like the data rates and ubiquity to make it really take off. Any plateau we reach will be a temporary one, followed by another exponential growth phase.

Sowa — While the Internet growth is slowing, the use of Internet II, VPNs, and the phenomena of social networking on Web 2.0, the emerging trends of Web 3.0 (see *IEEE Computer Magazine* 2008), and parallel computing, cloud-computing, and virtualization concepts will rapidly create new threats not yet envisioned or secured against. The greatest modes of attack on the Internet are currently based on vulnerabilities of existing software, but IEEE and CERT describe more dangerous vulnerabilities that still widely exist in routers, switches, internet protocols (IP), transmission control protocols (TCP), and Domain Name Services (DNS). These are the more dangerous threats that can be cultivated for true cyberwarfare attacks.

39. Technology is creating a knowledge-dependent global society.

More and more businesses, and entire industries, are based on the production and exchange of information and ideas rather than exclusively on manufactured goods or other tangible products. At the same time, manufacturers and sellers of physical products are able to capture and analyze much more information about buyers' needs and preferences, making the selling process more efficient and effective. The number of Internet users in the United States more than doubled between 2000 and 2007, to nearly 231 million, or 69 percent of the population. Yet the percent of the population online has remained almost unchanged since 2004. And while the percentage of

Internet users in China is smaller than in the U.S., the number of users there passed the U.S. early in 2008.

Assessment: This trend will not reach even its half-way mark until the rural populations of China and India gain modern educations and easy access to the Web.

Implications: This trend is raising the level of education required for a productive role in today's workforce. For many workers, the opportunity for training thus is becoming one of the most desirable benefits any job can offer.

Even entry-level workers and those in formerly unskilled positions require a growing level of education. For a good career in almost any field, computer competence is mandatory.

Knowledge workers are generally better paid than less skilled workers, and their proliferation may raise overall prosperity.

However, data and communications technologies also are exposing workers in the developed world to competition from low-wage countries. It is not yet clear at what pay level these competing forces will balance.

This trend also is enlarging the income gap between well educated workers and those with a high school degree or less. That gap will continue to grow.

In ten years, most digital devices will combine multimedia communication functions and real-time voice translation, so that conversations originating in one of seven or eight common languages can be heard in any of the others. These technologies will enable even more people to become knowledge workers or, at least, knowledge-enhanced workers.

Telecommuting will make many companies more efficient, cutting their expenses in the process. New technologies create new industries, jobs, and career paths, which can bring new income to developing countries. An example is the transfer of functions such as technical support, and more recently R&D, to Asian divisions and service firms.

For some developing countries, computer skills are making it faster and easier to create wealth than a manufacturing economy ever could. India, for example, is rapidly growing a middle class, largely on the strength of its computer and telecom industries. Other lands will follow its example.

Implications for Information Warfare and Operations: Increasing dependence on technology effectively translates to growing fragility. Disrupt essential information or communications systems, and a company, government agency, or military unit could be dead in the water, or at least cut off from oversight and coordination with its partners. Telecommuting systems, for example, offer several obvious opportunities to disrupt the operations of the company or agency that depends on them.

It is this trend that makes information warfare and operations such a vital component of future military operations and national security. These effects have been commented upon at some length in the other trend discussions.

Probability is 100 percent; impact is high.

Expert Comments:

Ayers — The "bunker-buster" ammunition that could be brought to bear within the context of cyberwar has not yet been deployed (or at least apparently not yet in a manner that has worked well.) How knowledge-dependent populations react—or how "new media" societies are capable of reacting—when such weapons are deployed, may ultimately determine their fate.

The chaos that could be caused either under a limited (homemade) EMP scenario or as a result of one or more high-altitude nuclear blasts would be devastating to a Western population in many ways. The losses incurred would make the current economic downturn seem like a mere irritant. Obtaining long-term assistance—whether in the form of backup electronics and parts, or merely food, water, and shelter—would be difficult even if only for a relatively small region within the continental United States.

Even if deaths caused by a loss of power to medical technology were discounted, an indirect casualty list would eventually begin to grow—especially if EMP attack(s) were wide-scale. Homelessness could probably be limited, but exposure to extreme heat or cold and a lack of clean water, food, and simple survival skills would be highly evident. A large portion of the U.S. population would no longer have access to printed material for survival assistance, as many have discarded books in favor of databases available via the Internet. The fact that localized EMP weapons would most probably be used in major cities (and of course deployed without warning) would complicate matters enormously, as hunting (for food) would be unlikely, unless it were for small rodents or other city-dwelling animals.

Coates — Many regions of the world, either neutral or favorable to us, may be victimized by IW, cyberwar, and we may therefore need to look at how to assist them, at this stage generically; later, specifically.

The problem is open as to how we might assist our long term allies, e.g., the UK, should it undergo an IW attack.

Kapinos — It is important to consider that there is likely to be a strong relationship between cyber-crime and cyber warfare. Coming from the perspective of the Law Enforcement community, and working as a strategic planner within that community — I continually stress that much of the crime that we will be faced with in the future will be electronic in nature (cyber crime.) In his famous 1970 novel *The Godfather*, Mario Puzo said that "a good lawyer with a briefcase can steal more than a hundred men with guns". Today, I would paraphrase that to say that an inventive hacker with a laptop can

steal more than a hundred lawyers with briefcases. Certainly, one of the things that could be stolen, altered or destroyed is information of all sorts.

I would also suggest that cyber-criminals (even seemingly innocuous ones) pose a potentially much greater threat than many believe. Through routine systems hacking, petty electronic theft, etc, these operators gradually build skill sets and learn and refine techniques that can make them valuable assets to those with more comprehensive plans. Small electronic information thefts or hacking-induced mischief can serve as a means to explore and test the vulnerabilities of large data repositories or control systems. Even the teenager who uses his computer talent to produce fake driver's licenses for his friends to drink underage is developing abilities that can be later put to use in forging false ID documents to facilitate security breaches.

With this in mind, I believe that it is crucial for the law enforcement and intelligence communities to work in concert to identify, and address the sources of cyber threats. All law enforcement agencies must develop the capability to properly investigate all types of electronic crime. Information on such activity must be regularly shared between agencies at the local, state and federal levels through the fusion center process. We do well at this here in Northern Virginia, but this process must become the norm nationwide.

LaDuke — By its nature, knowledge is one. We know this because everything we know can be categorized and all categories can be further categorized. Technology is a connective force to bring together knowledge into one, through increases in capabilities like processing, storage, communication, connectivity, collaboration, etc.

Expertise opposes knowledge coming together because it is more about (political) status than logic. It is a status-based, not logic-based judgment of who knows. This scales up to an educational political system and then to a world political system that make status-based, sometimes logical, judgments. Status-based judgment opposes knowledge coming together into one because factions are inherent to this kind of reasoning. Any form of separation of knowledge (into two, or three, or 300 social knowledge bases) creates knowledge factions. These factions polarize just like physical nation states do and form the basis of knowledge wars.

The current social order of knowledge working based on expertise, political factions, and physical boundaries is on a collision course with the fundamental nature of knowledge. As we rise toward ubiquitous computing, this conflict will become more and more apparent.

Pearson — Yes, very dangerous, but not as dangerous as trying to live without it.

Rowlatt — Possible consequences to our existing approaches to cyber threats may include:

Counter measures to cyber threats developed by us, will impede our ability to work effectively let alone efficiently. Firewalls, authentication, and encryption programs have the potential to slow the flow of information. An enemy would love to slow down some decision cycles. This approach would allow them to achieve the aim simply by presenting a threat be it credible or virtual.

We become distrustful of information contained or processed within cyber networks.

Sowa — Our existing high-priced cyber-system remains extremely fragile and vulnerable to grave systemic attacks. Our main defenses are based at the perimeter. These defenses will continue to minimize access, and thereby thwart common attacks well into the future. Newly found TCP-IP and DNS threats; switch and router threats; as well as threats caused by poorly-determined and thought-out approaches by vendors (i.e., client-based server control, etc.) will continue to propagate vulnerabilities and security risks. Smart phones, sub-netbooks, PDA's, wearables, RFID technology, and nano-technologies that can alter clothing fabric into computer storage units—will continue to alter the technical threats that have to be foreseen and planned for.

Steele — A single dominant nation-state is a declining reality. The rise of the "cyber state" —potentially cyber created and maintained existing in cyberspace (without geopolitical boundaries—without a label "China, Asia, North America, etc.") will join the collection of geopolitical nations.

Thomas — Departure from a global village to a segmented society: There are now thousands of specific sites on the Internet for ideologies of all types which, at the moment, have done as much to divide nations as to integrate them.

ENVIRONMENTAL TRENDS

40. People around the world are becoming increasingly sensitive to environmental issues as the consequences of neglect, indifference, and ignorance become ever more apparent.

The World Health Organization (WHO) estimates that 3 million people die each year from the effects of air pollution, about 5 percent of the total deaths. In the United States, an estimated 64,000 people a year die of cardiopulmonary disease caused by breathing particulates. In sub-Saharan Africa, the toll is between 300,000 and 500,000 deaths per year. Pollution-related respiratory diseases kill about 1.4 million people yearly in China and Southeast Asia. And contaminated water is implicated in 80 percent of the world's health problems, according to WHO. An estimated 40,000 people around the world die each day of diseases directly caused by contaminated water, more than 14 million per year.

Though some debate remains about the cause, the fact of global warming has become undeniable. At Palmer Station on Anvers Island, Antarctica, the average annual

temperature has risen by 3 to 4 degrees since the 1940s, and by an amazing 7 to 9 degrees in June—early winter in that hemisphere.

Anticipating a three-foot rise in sea levels, the Netherlands is spending $1 billion to build new dikes.

Assessment: A solid majority of voters throughout the developed world, and even some in the developing lands, now recognize the need to clean up the environment, and especially to control greenhouse warming. They will keep this trend intact for at least the next 30 years.

Implications: Throughout most of the world, polluters and private beneficiaries of public assets will increasingly confront restrictive regulations designed to serve the interests of the community at large.

CO2 will remain a problem for many years to come. If air pollution were halted instantly, it would take an estimated 200 years for carbon dioxide and other greenhouse gases to return to pre-industrial levels.

Impurities in water will become an even greater problem as the population of the developed countries ages and becomes more susceptible to infectious diseases.

Recent analyses say there is a 90 percent chance that the planet's average annual temperature will rise between 3 and 9 degrees Centigrade over the next century. This will cause severe dislocations both for plant and animal populations and for many human activities.

Environmental policies will provoke a political backlash wherever they conflict with entrenched interests, as they have long done in the American West.

Implications for Information Warfare and Operations: None have been recognized.

Expert Comments:

Pearson — This could be a relatively short-lived passion though, people just don't have the energy to stay annoyed at something forever. And less so the commitment to do something about it for any duration. But this doesn't matter much because there are some trigger points in environmental decay and if we pass them, we're stuffed. If we get past them safely, we won't need to worry any more.

Sowa — So far, we've associated high threats to technology or network-based signal or social attacks. Such attacks assume that the threat is technologically-inclined. But, a greater terrorist threat may actually be low tech—based on putting a component of cyberspace out of action, or by overloading it destructively. Such a low-tech environmental threat, for example, could be environmentally, or chemically contaminating server rooms and tier one routing centers.

If a mainline center were breached in such a manner, you wouldn't have to attack the energy transmission input, or the network—but you could totally or purposefully disrupt the system.

Such an attack would start with the planting of a worm or Trojan horse in the system that could be remotely activated. If we were to upgrade our infrastructures, for example, or outsource it to less controlled global environments, it is not unthinkable that such a breach could occur—even passively, months before the attack. The second step would be to launch an environmentally altering attack on the center, forcing it to be evacuated. With no capability to get to the center, or the monitors—a cyber-attack could be activated that could not be easily defended against.

Off-site monitoring, or systemic switchover, creates more vulnerabilities, and can release systemic problems that cold have otherwise been contained.

41. Water shortages will be a growing problem for much of the world. In many regions, they are severe already.

The northern half of China, home to perhaps half a billion people, already is short of water. The water table under Beijing has fallen nearly 200 feet since 1965. Australia's Murray-Darling river system, which supplies water for 40 percent of the country's crops and 80 percent of its irrigation, no longer carries enough water to reach the sea without constant dredging. Salinity in the Murray is rising so quickly that the water is expected to be undrinkable in 20 years. There is worse to come. According to U.N. studies, at least 3.5 billion people will run short of water by 2040, almost ten times as many as in 1995. Ten years later, fully two-thirds of the world's population could be living in regions with chronic, widespread shortages of water.

Assessment: This trend will remain with us for the very long term.

Implications: Providing adequate supplies of potable water will be a growing challenge for developing and developed countries alike.

Such problems as periodic famine and desertification can be expected to grow more frequent and severe in coming decades.

In many lands, including parts of the United States, growing water shortages may inhibit economic growth and force large-scale migration out of afflicted areas.

Climate change is expected to reduce the flow of Australia's parched Murray River by a further 5 percent in 20 years and 15 percent in 50 years.

Water wars, predicted for more than a decade, are a threat in places like the Kashmir: much of Pakistan's water comes from areas of Kashmir now controlled by India.

Other present and future water conflicts involve Turkey, Syria, and Iraq over the Tigris and Euphrates; Israel, Jordan, Syria, and Palestine over water from the Jordan River and the aquifers under the Golan Heights; India and Bangladesh, over the Ganges and Brahmaputra; China, Indochina, and Thailand, over the Mekong; Kyrghyzstan, Tajikistan, and Uzbekistan over the Oxus and Jaxartes rivers; and Ethiopia, Sudan, and at least six East African countries, including Egypt, over the Nile.

In the United States, repair of decayed water systems is likely to be a major priority for older cities such as New York, Boston, and Atlanta. Cost estimates for necessary replacement and repair of water mains range up to $1 trillion.

Implications for Information Warfare and Operations: By raising tensions between neighbors in the developing world, water shortages may encourage the development of active cyber-warfare programs in countries that formerly would not have thought them necessary.

Probability is 35 percent; impact is low. In less developed countries, information warfare attacks will not be common, because local infrastructures seldom depend sufficiently on technology to make them effective. Simple “land grab” and traditional military attacks will be.

Expert Comments:

Forster — Water has often been the source of inter-state conflict and continues to threaten stability in many regions. Furthermore, modern societies rely on water systems that transport fresh water (Singapore-Malaysia for example) and sewage treatment facilities. These systems are vulnerable to cyberattacks. Deprivation of water resources as a result of an attack would have significant social and economic impacts as well as potentially igniting inter-state conflict.

Pearson — If solar power can be developed cheaply enough, then desalination becomes more of an alternative for many areas. Pipelines will be needed in some areas.

42. Recycling has delayed the “garbage glut” that threatened to overflow the world’s landfills, but the problem continues to grow.

Americans now produce about 4.5 pounds of trash per person per day, twice as much as they threw away a generation ago. Seventy percent of U.S. landfills will be full by 2025, according to the EPA. Japan expects to run out of space for industrial waste as soon as 2008 and for municipal solid waste by 2015. In London and the surrounding region, landfills will run out of room by 2012.

Recycling has proved to be an effective alternative to dumping. As of 2005, Germany recycled 60 percent of its municipal solid waste, 65 percent of manufacturing waste, 80 percent of packaging, and 87 percent of construction waste, according to the

Environment, Nature Conservation, and Nuclear Safety. Largely as a result, the number of landfills for domestic waste has been reduced from about 50,000 in the 1970s to just 160.

Assessment: The challenge of dealing with garbage will grow for so long as the world's middle classes continue to expand or until technology finds ways to recycle virtually all of the materials used in manufacturing and packaging. This trend will remain intact through at least 2050.

Implications: Recycling and waste-to-energy plants are a viable alternative to simply dumping garbage. This trend will push the development of so-called life-cycle design, which builds convenient recyclability into new products from their inception.

Expect a wave of new regulations, recycling, waste-to-energy projects, and waste management programs in the United States and other countries in an effort to stem the tide of trash. In the United States, it will of course begin in California, a jurisdiction often cited by policy forecasters as a bellwether of change.

State and local governments will tighten existing regulations and raise disposal prices in Pennsylvania, South Carolina, Louisiana, and other places that accept much of the trash from major garbage producers such as New York. Trash producers in the developed world will ship much more of their debris to repositories in developing countries. This will inspire protests in the receiving lands.

Beyond 2025 or so, the developing countries will close their repositories to foreign waste, forcing producers to develop more waste-to-energy and recycling technologies. Ultimately, it may even be necessary to exhume buried trash for recycling to make more room in closed dump sites for material that cannot be reused.

Waste-to-energy programs will make only a small contribution to the world's growing need for power.

Implications for Information Warfare and Operations: None have been identified.

Expert Comments:

Pearson — There are now mountains of stuff waiting to be recycled, and no buyers. We need new solutions. Environmental activists are a rapidly growing terrorist threat who have highly dangerous pseudo-religious mindsets.

43. Preference for industrial development over environmental concerns is fading slowly in much of the developing world.

The Pew Research Center reports that less than one-fourth of respondents in any African country rated environmental problems as the world's most important threat. In Ethiopia, where desertification is at its worst and drought is a constant threat, only 7

percent did so. Beijing has made repairing the environment a national priority. Yet 70 percent of the energy used in China comes from coal-burning power plants, few of them equipped with pollution controls. The country intends to build over five hundred more coal-fired plants in the next ten years. Even Germany has committed to building more power plants fired by high-sulfur brown coal.

Assessment: View this as a counter-trend to Trend 40. It will remain largely intact until the poor of India and China complete their transition into the middle class, around 2040.

Implications: Broad regions of the planet will be subject to pollution, deforestation, and other environmental ills in the coming decades.

Acid rain like that afflicting the United States and Canada will appear wherever designers of new power plants and factories neglect emission controls.

In India, an area the size of the United States is covered by a haze of sulfates and other chemicals associated with acid rain. Look for this problem to appear in most other industrializing countries.

Diseases related to air and water pollution will spread dramatically in the years ahead. Already, chronic obstructive pulmonary disease is five times more common in China than in the United States. As citizens of the developing countries grow to expect modern health care, this will create a growing burden on their economies.

This is just a taste of future problems, and perhaps not the most troublesome. Even the U.S. government now admits that global warming is a result of human activities that produce greenhouse gases. It now seems that China and India soon will produce even more of them than the major industrialized nations. Helping the developing lands to raise their standards of living without creating wholesale pollution will require much more aid and diplomacy than the developed world has ever been willing to give this cause.

Implications for Information Warfare and Operations: New computer controlled factories, power stations, pipelines, and other industrial facilities will expose many developing countries to the same kind of technological disruption previously faced only by the industrialized world.

Probability is 65 percent; impact is low to medium.

Expert Comments:

Pearson — This may reduce potential for recovery from recession and lead to long term decline relative to other nations.

44. Concern over species extinction and loss of biodiversity is growing quickly.

An estimated 50,000 species disappear each year, up to 1,000 times the natural rate of extinction, according to the United Nations Environmental Program. By 2100, as many as half of all species could disappear. Eleven percent of birds, 25 percent of mammals, and 20 percent to 30 percent of all plants are estimated to be nearing extinction. Some 16,118 species are now listed as threatened (7,925 animal species and 8,393 plant and lichen species), according to the 2006 Red List of the International Union for Conservation of Nature and Natural Resources. This is an increase of nearly 2,700 in four years. The real list is likely much larger, as the group has evaluated only 40,000 of the 1.5 million species on its list. The chief cause for species loss is the destruction of natural habitats by logging, agriculture, and urbanization.

Assessment: This trend has at least three decades to run.

Implications: Saving any significant fraction of the world's endangered species will require much more effort and expense than many governments find acceptable. For species such as corals, if the loss is attributable largely to climate change, it may not be possible.

Species loss has a powerful negative impact on human wellbeing. Half of all drugs used in medicine are derived from natural sources, including fifty-five of the top one hundred drugs prescribed in the United States. About 40 percent of all pharmaceuticals are derived from the sap of vascular plants. So far, only 2 percent of the 300,000 known sap-containing plants have been assayed for useful drugs. Most of the species lost in the years ahead will disappear before they can be tested.

The Indonesian economy loses an estimated $500,000 to $800,000 annually per square mile of dead or damaged reef.

Australia may lose even more as degradation of the Great Barrier Reef continues. The U.N. Intergovernmental Panel on Climate Change predicts that the Reef will be "functionally extinct" by 2030.

Diverse ecosystems absorb more carbon dioxide than those with fewer species. Loss of biodiversity thus is a potential cause of global warming.

Implications for Information Warfare and Operations: If this trend carries significant implications for this field, they are remarkably obscure.

Expert Comments:

Pearson — Progress in biotech will now accelerate and lead to optimism about recovering lost species. We will then see synthetic biology kick in, offering to create new species, and potential for Gaia 2.0. Many weapons technologies could be built under the guise of benign biotech.

Sowa — The trend of biotechnology developing cellular computers has been discussed in *Scientific American*, *Science Magazine*, and *Discover*. These are results created within genome and nano-technological research labs. Such a computer will not be programmed or behave like the electronic and electrical systems we now defend. This trend needs to be discussed as an emergent concept—but its impact, short term, is obscure.

45. Urbanization, arguably the world's oldest trend, continues rapidly.

Forty-eight percent of the world's population currently lives in cities, according to the Population Reference Bureau's 2006 World Population Data Sheet. By 2030, that will grow to 60 percent, as some 2.1 billion people are added to the world's cities.

Cities are growing fastest in the developing world. In 1950, there were just eight megacities, with populations exceeding 5 million, in the world. By 2015, there will be fifty-nine megacities, forty-eight of them in less developed countries. Of these, twenty-three will have populations over 10 million, all but four in the developing lands.

Natural increase now accounts for more than half of population increase in the cities; at most, little more than one-third of urban growth results from migration.

Assessment: After surviving for some 3,500 years, this trend is unlikely to disappear in the next 50.

Implications: Cities' contribution to global warming can only increase in the years ahead. As the world's supply of potable water declines, people are concentrating in those areas where it is hardest to obtain and is used least efficiently. This trend will aggravate water problems for so long as it continues. Many more people will die due to shortages of shelter, water, and sanitation. Epidemics will become still more common as overcrowding spreads HIV and other communicable diseases more rapidly.

Since urban growth is now due more to natural increase than to migration, programs designed to encourage rural populations to remain in the countryside may be misplaced.

Education and family planning seem more likely to rein in the growth of cities.

Implications for Information Warfare and Operations: As populations concentrate in cities, they become more dependent on distant manufacturers, farmers, and utilities, and on the transportation and communications systems that deliver products and information from outside. All the elements required to support urban life depend increasingly on technologies that are susceptible to disruption. This vulnerability will grow as society in general becomes ever more dependent on the expanding capabilities of technology. It represents an opportunity to undermine a country's capacity to wage war even without facing its troops.

Probability is 65 percent; impact is low. The impacts on population centers of direct cyber-warfare, as opposed to more traditional means, will be limited except in special circumstances. The possible use of information operations to attack food supplies, utilities, etc., has been documented in other trends.

Expert Comments:

Forster — The increased concentration of populations in cities increases the impact of any cyberattack and ranges from economic loss resulting from infrastructure failure or denial of services to potentially high loss of life resulting from a multitude of technology related incidents including the minaturization of highly destructive weapons to the release of bioweapons.

Pearson — It just needs one major plague to reverse this trend.

Sowa — The trend of urbanization and it vulnerabilities is discussed well here.

MANAGEMENT TRENDS

46. More entrepreneurs start new businesses every year.

In the United States, about 9 percent of men and 6 percent of women are self-employed. These fractions have been growing in about two-thirds of the OECD countries. Many women are leaving traditional jobs to go home and open businesses, even as they begin a family. At least half of the estimated 10.6 million privately held firms in the United States are owned by women, employing 19.1 million people and generating $2.46 trillion in sales annually.

For the 14 years ending in 2003, the most recent period for which data is available, small businesses (those with less than five hundred employees) created 92 percent of the net new jobs in the United States, according to the Census Bureau. The smallest companies, those with fewer than twenty employees, created 85 percent. However, jobs also disappear fastest from small companies, which are much more likely to fail than larger concerns. Though big-company layoffs have gotten the most publicity in the current recession, losses from smaller firms are likely to be even more severe.

Assessment: This is a self-perpetuating trend, as all those new service firms need other companies to handle chores outside their core business. It will remain with us for many years, not only because it suits new-generation values but because it is a rational response to an age in which jobs can never be counted on to provide a stable long-term income.

Implications: It is driven as well by the attitudes and values of Generation X and the Millennials and by the rapid developments in technology, which create endless opportunities for new business development.

Specialty boutiques will continue to spring up on the Internet for at least the next 15 years.

This trend will help to ease the poverty of many developing countries, as it already is doing in India and China.

Implications for Information Warfare and Operations: Where potential conflicts can be anticipated in the long term, companies can be "planted" in such fields as network communications and security. Building up contacts and contracts over a period of years, they can eventually be well placed to disrupt critical technology systems in time of need.

Conversely, foreign-born entrepreneurs in the United States and Europe could be of significant use to extremist adversaries from their homelands. Even if they are unsympathetic to the extremist cause, they may be susceptible to threats or pressure affecting their relatives at home.

Probability is 50 percent; impact is low.

Expert Comments:

Kapinos — This trend and the next are related, and they can have both good and bad implications. One positive that I see in the entrepreneurial and networked management businesses is — fewer critical capabilities and information assets are centralized in one place, or under the control of one firm. This can be valuable in ensuring the recoverability from a significant system crash or disruption. With more assets capable of stepping in to repair the damage (even in combination with each other), the quicker a new usable system could regenerate. The idea is that with many nodes in place, knocking any one or two out will not destroy the system: the system can rebuild around the damaged nodes more easily.

Pearson — Yes, lots of traditional industries will be challenged by new models, and some won't survive, notably the music industry. We will get all the music we want, but will lose most or all of the big traditional players.

47. Horizontal "connect-and-collaborate" organizations are quickly displacing the old hierarchical command-and-control model of management.

The typical large business has reshaped itself or is struggling to do so. Soon, it will be composed of specialists who rely on information from colleagues, customers, and headquarters to guide their actions.

Upper management is giving fewer detailed orders to subordinates. Instead, it sets performance expectations for the organization, its parts, and its specialists and supplies the feedback necessary to determine whether results have met expectations.

Assessment: This is a well-established trend. At this point, many large corporations have restructured their operations for greater flexibility, but many others still have a long way to go.

This trend will continue in the United States for at least the next 15 years. The developing world may largely bypass this step in its new organizations and go straight to networked management structures.

Implications: This management style suits Generation Xers and Millennials well, as it tends to let them work in whatever fashion suits them so long as the job gets done.

Downsizing has spread from manufacturing industries to the service economy. Again, this process encourages the entrepreneurial trend, both to provide services for companies outsourcing their secondary functions and to provide jobs for displaced employees.

Many older workers have been eliminated in this process, depriving companies of their corporate memory. Companies have replaced them with younger workers whose experience of hard times is limited to the relatively mild recession since 2000. Many firms may discover that they need to recruit older workers to help them adapt to adversity.

This too is driving the entrepreneurial trend. Many older workers find themselves self-employed by default, as they need income and cannot find work in their accustomed fields.

Implications for Information Warfare and Operations: These companies are highly dependent on computerized accounting and operations software and on computerized communications with their suppliers and clients. Some even grant broad access to their ordering, inventory, and manufacturing control systems. This creates obvious vulnerabilities that could be of use in cyber warfare.

Probability is 65 percent; impact is medium. While a single event will have limited results, the huge number of targets will provide rich “hunting grounds” for economic terrorism utilizing information warfare.

Expert Comments:

Ayers — Perhaps the most recent example of the extent to which information-based managerial models have taken over (at least conceptually) was seen with the transition of power between Presidents Bush and Obama. President Obama has been hailed as “the first wired president” (see Pete Yost’s Associated Press article “The Wired President: Obama creates an e-mail trail” as reprinted on Forbes.com [23 January 2009]), and his staff was reportedly aghast at the lack of up-to-date technology within the White House (see Anne Komblut’s “Staff Finds White House in the Technological Dark Ages,” *The Washington Post* [22 January 2009].) Although irritated by setbacks in

the flow of communications, the incoming team apparently recognized that archival and security needs dictated the resources used—at least for the moment. Whether or not that will continue to be the case has yet to be seen. One thing is sure—the President of the United States is a prime target for anyone wishing to engage in cyberwar.

Forster — Greater damage is done by a cyberattack on these kind of organizations.

One social trend that I think is missing is the erosion of socialization that is occurring as technology proliferates. Reliance on text messaging is perverting the English language and discouraging face-to-face personal interaction. geographically dispersed workforce including people working at home is reducing the informal communication and socialization mechanisms that helped development organizational loyalty, purpose, and personal commitment to a group. Impromptu discussions in the hallway or around the "watercooler" are disappearing. The result is less development of an organizational culture and commitment, less transfer of knowledge to successors, and perhaps a decline in innovation that results from group discussions around a subject or the immediate learning from a situation.

Kapinos — See Trend 46.

LaDuke — Networks allow groups to distribute intention. When that intention is hostile and aligned, this creates a distributed fighting force. Communication enables this distributed intention and as such is the backbone of militant Islam.

Intelligence technology of the future will have three main fronts:

1. The traditional approach of communication interception,
2. Threatening intention detection through technology and
3. influence or persuasion to change intention.

Pearson — Informal organisations will flourish, expedited by too intense legislation. Administrative burdens already force some people to work together as freelancers instead of having an employer/employee relationship.

Sowa — This creates a very "target-rich" vulnerable society—making disruption tactics and planted cells highly likely.

48. As 0rganizations simplify their structures, they are squeezing out personnel.

Computers and information-management systems have stretched the manager's effective span of control from six to twenty-one subordinates. Information now flows from frontline workers to higher management for analysis. Thus, fewer mid-level managers are needed, flattening the corporate pyramid.

The span of control could stretch again if computer science finally delivers on its long-delayed promise of artificial intelligence. Opportunities for advancement are shrinking, because they come within the worker's narrow specialty, rather than at the broader corporate level. By 2001, only one person in fifty was promoted, compared with one in twenty in 1987.

Assessment: In the United States, downsizing, restructuring, reorganization, and cutbacks of white-collar workers will continue at least through 2025. Its pace will not slow unless technology ceases to deliver new ways to replace human workers with faster, cheaper, more reliable hardware and software.

Implications: The current recession will be filled by another "jobless recovery" as companies squeeze still more productivity out of their existing workforce, rather than hiring new employees.

A typical large business in 2015 will have fewer than half the management levels of its counterpart in 1995, and about one-third the number of managers.

Information-based organizations have to make a special effort to prepare professional specialists to become business leaders. Broad experience of the kind needed by a CEO no longer comes naturally during an executive's career.

Top managers must be computer-literate to retain their jobs and must make sure to oversee the increased spans of control that computers make possible.

Finding top managers with the broad experience needed to run a major business already has become difficult. It can only grow more so as the demand for specialization grows. This will reduce promotion from within and encourage companies to seek upper-level execs from other firms, and even industries.

Executives increasingly will start their own companies, rather than trusting the old-fashioned corporate career path to provide advancement.

Ultimately, this trend will require a wholesale rethinking of the social contract, as it becomes difficult or impossible to create enough fulfilling, well paid jobs for human workers to support the population. The end of salaried work is not yet near, but it could arrive within the lifetimes of today's younger generations.

Implications for Information Warfare and Operations: This trend too increases corporate vulnerability to assaults that compromise their high-tech support systems. A similar effect may well be seen in many government departments as tax revenues decline in the current recession and stimulus programs run up deficits that make it difficult to fund ordinary operations, much less to pay for new initiatives.

Probability is 65 percent; impact is medium. While a single event will have limited results, the increasing number of companies with limited and/or key personnel will provide rich “hunting grounds” for economic terrorism utilizing information warfare.

Expert Comments:

Pearson — Yes, and new ones will never take on the staff in the first place. This will prevent governments from forcing through legislation on employment rights, gender equality, etc.

Sowa — This also creates a very “target-rich” vulnerable society—making disruption tactics and planted cells highly likely.

49. Government regulations will continue to take up a growing portion of the manager’s time and effort.

In 1996, the U.S. Congress passed regulatory reform laws intended to slow the spread of government regulations. Nonetheless, by 2001 more than 14,000 new regulations were enacted. Not one proposed regulation was rejected during this period. The Brussels bureaucrats of the European Union are churning out rules at an even faster rate, overlaying a standard regulatory structure on the national systems of member countries.

This is not all bad. A study by the Congressional Office of Management and Budget estimated that major federal regulations enacted in the decade ending September 2002 cost between $38 billion and $44 billion per year. However, the estimated benefits added up to between $135 billion and $218 billion annually.

Assessment: If the future holds an end to this trend, it is not yet in sight.

Implications: Regulations are necessary, unavoidable, and often beneficial. Yet it is difficult not to see them as a kind of friction that slows both current business and future economic growth.

The proliferation of regulations in the developed world could give a competitive advantage to countries such as India and China, where regulations that impede investment and capital flow are being stripped away, and health, occupational safety, and environmental codes are still rudimentary or absent.

However, there is a significant penalty for the kind of risk that comes from inadequate regulation. China pays an estimated risk penalty of 6.49 percent for international borrowing. Per capita GDP, access to capital, foreign direct investment, and other measures of a country’s economic health all decline directly with a rising Opacity Index, which is heavily influenced by the lack of effective regulations to guarantee a level playing field for those doing business there. As a result, lands such as Russia will

remain at a competitive disadvantage until they can pass and enforce the regulations needed to ensure a stable, fair business environment.

Implications for Information Warfare and Operations: In light of the widespread vulnerability of corporate computer networks and the Internet, some of the coming regulations may be intended to tighten security.

Probability is 35 percent; impact is low.

Expert Comments:

Pearson — And therefore expedite the move to non-company working. Freelancing will dominate many industries, apart from the most capital-intensive.

Sowa — Regulation of networks globally is expected to increase dramatically within the next 20 years. The ramifications mean that cyberwarfare strategists will have to learn how to improvise, adapt, and overcome problems caused by these changes, or work to better anticipate problems such runaway regulation will have on carrying out their objective—and they will need to maintain a voice through the regulatory process.

INSTITUTIONAL TRENDS

50. Multinational corporations are unifying the world and growing more exposed to its risks.

The continuing fragmentation of the post-Cold War world has reduced the stability of some lands where government formerly could guarantee a favorable—or at least predictable—business environment. The current unrest in Iraq is one example. One risk now declining is the threat of sudden, extreme currency fluctuations. In Europe, at least, the adoption of the euro is making for a more stable financial environment.

Assessment: This trend will continue for at least the next 30 years, as companies in the developing world diversify into less developed markets.

Implications: It is becoming ever more difficult for business to be confident that decisions about plant location, marketing, and other critical issues will continue to appear wise even five years into the future. All long-term plans must include an even greater margin for risk management. This will encourage outsourcing rather than investment in offshore facilities that could be endangered by sudden changes in business conditions.

Countries that can demonstrate a significant likelihood of stability and predictable business outcomes will enjoy a strong competitive advantage over neighbors that cannot. Witness the rapid growth of investment in India now that deregulation and privatization have general political support, compared with other Asian lands where conditions are less predictable.

Although Russia has continued to attract Western investment, particularly in its energy industry, increasingly autocratic governance by the Putin regime and any successors could eventually discourage foreign companies from doing business there or require much more favorable terms to justify accepting the associated risks.

Major corporations also can help to moderate some risks in unstable countries by threatening to take their business elsewhere.

Implications for Information Warfare and Operations: Overseas divisions of multinationals may offer antagonists a means of entering American "cyberspace" without ever having to cross the national boarder: Just get a job working with the computers at an American-owned company.

Probability is 50 percent; impact is low to medium.

Expert Comments:

Pearson — They are also becoming more of a target for anyone trying to push any cause.

Sowa — This has already been discussed at length. Multinationals create a very "target-rich" vulnerable society—making disruption tactics and planted cells highly likely.

51. Consumers increasingly demand social responsibility from companies and each other.

Companies increasingly are being judged on how they treat the environment, their workers, and their customers. Many are changing their business practices as a result. For example, home-improvement retailers Home Depot and Lowe's have stopped buying wood from countries with endangered forests, while Nike now publishes its discoveries of worker abuse by offshore suppliers. Costco offers much better benefits than its competitors and has half the employee turnover rate as a result. In a 2005 survey of nearly 1,200 companies, 81 percent— and 98 percent of large firms—said corporate citizenship is a priority; 84 percent said that being socially responsible has improved profits. Once the business-friendly Bush administration leaves Washington, government intervention will rebound in sectors from finance to industrial chemicals. To avoid political backlash from the right, regulation is likely to be carefully targeted and limited, at least for a time.

Assessment: This trend is well established in the industrialized world, but only beginning in the developing world. It can be expected to grow more powerful as the no-nonsense, bottom-line-oriented Generation Xers and Millennials gain influence.

Implications: Once the current, business-friendly administration leaves Washington, government intervention will supplant deregulation in the airline industry (in the interest

of safety and services), financial services (to control instability and costs), electric utilities (nuclear problems), and the chemical industry (toxic wastes.)

In the United States, frequent incidents of political corruption may spread the demand for greater responsibility into the field of government and public service, although that is not yet clear. As the Internet spreads Western attitudes throughout the world, consumers and environmental activists in other regions will find more ways to use local court systems to promote their goals. Litigation is likely to become a global risk for companies that do not make the environment a priority.

Implications for Information Warfare and Operations: None are noted.

Expert Comments:

Pearson — But only if it doesn't increase prices too much. The market still rules.

52. On average, institutions are growing more transparent in their operations, and more accountable for their misdeeds.

Many different forces are promoting this change in various parts of the world. In the United States, the wave of business scandals in 2004, the exposure of child abuse within the Catholic Church, and other perceived offenses by large organizations have inspired demands for greater transparency and accountability. China, rated by Kurtzman Group as the most opaque of the major nations, was forced to open many of its records as a precondition for joining the World Trade Organization. In India, a country often regarded as one of the world's most corrupt, the Central Vigilance Commission has opened the country's banking system to more effective oversight. Lesser "vigilance commissions" now oversee many parts of the Indian economy and government. More generally, wars against terrorism, drug trafficking, and money laundering are opening the world's money conduits to greater scrutiny. They also are opening the operations of nongovernmental organizations that function primarily as charitable and social-service agencies but are linked to terrorism as well.

Assessment: There are roughly as many reactions against this trend as there are governments, agencies, and individuals with something to hide. Yet, the benefits of transparency are so clear that the general decline of barriers to oversight is likely to continue until societies develop a consensus about how much—or little—secrecy is really necessary. We give this trend at least 20 years of continued vigor.

Implications: Countries with high levels of transparency tend to be much more stable than more opaque lands. They also tend to be much more prosperous, in part because they find it easier to attract foreign investment.

Greater transparency reduces the operational effectiveness of the world's miscreants. It impedes drug traffickers and terrorist organizations, as well as dishonest governments and corrupt bureaucrats.

Implications for Information Warfare and Operations: Transparency easily equates to vulnerability. Whatever law-abiding Americans know or can learn about a company's operations, less benign observers can learn as well.

Probability is 45 percent; impact is low. Corporate security personnel generally understand the vulnerabilities that accompany transparency, and most companies are taking steps to minimize them while remaining as open as their circumstances require. Many of these measures will close vulnerabilities to social engineering.

Expert Comments:

Pearson — They are just getting better at hiding them, having informal chats instead of formal meetings, and chatting in a corridor rather than sending emails that can be tracked. Companies and regulators are actually left with less power, not more.

Sowa — Transparency opens the door to social engineering and maneuvering to achieve cyber-attack goals. The vulnerabilities are often understood—as stated above. Only a custom response will work here.

53. Institutions are undergoing a bimodal distribution: the big get bigger, the small survive, and the mid-sized are being squeezed out.

Economies of scale enable the largest companies to win out over mid-sized competitors, while "boutique" operations can take advantage of niches too small to be efficiently tapped by larger firms. We see the result in a wide range of industries throughout the developed world. In agriculture, banking, auto manufacturing, telecommunications, and many other sectors, the largest firms have been buying up their mid-sized competitors or driving them out of business. At the same time, hundreds or thousands of tiny operators have arisen in each industry to get rich by serving markets beneath the notice of the giants.

Assessment: Thanks in part to technology, this trend is likely to be a permanent feature of the business scene from now on.

Implications: No company is too large to be a takeover target if it dominates a profitable market or has other features attractive to profit-hungry investors. No niche is too small to attract and support at least one or two boutique operations. Thus far, industries dominated by small, regional, often family-owned companies have been relatively exempt from the consolidation now transforming many other businesses. Takeovers are likely even in these industries in the next decade.

This consolidation will extend increasingly to Internet-based businesses, where well-financed companies are trying to absorb or out-compete tiny online start-ups, much as they have done in the brick-and-mortar world.

However, niche markets will continue to encourage the creation of new businesses. In Europe as of 2006, no fewer than forty-eight small, no-frills airlines in twenty-two countries had sprung up to capture about 28 percent of the Continental market share. Only fifteen offered more than fifty flights per day.

Implications for Information Warfare and Operations: This trend is concentrating growing numbers of critical business functions into a shrinking pool of corporate networks and headquarters. For example, a "cyberstalker" targeting Washington Mutual in July 2008 now might easily have access to JP Morgan Chase as well. To a degree we cannot yet quantify, this trend may make the West more susceptible to information warfare.

By increasing the size of institutions, this trend also increases the likely impact of an attack on one of them. If, say, the world contained 20 large banks a decade ago but has only ten now, disrupting one of them is likely to cause a much greater shock to the financial markets than it would have done in the past.

Probability is 95 percent; impact is medium. Bigger targets means more "bang for the buck" from a given attack. However, this kind of consolidation also reduces the supply of potential targets, and the remaining targets are likely to be better hardened. Yet, the probability of simple, exploitable mistakes on the part of the target goes up exponentially with the size of the organization.

Expert Comments:

Kapinos — This is the reverse of the trend above and demonstrates the vulnerability of systems concentrated in the hands of relatively few operators. This trend increases the risk of disruption. Trends 46 and 47 both suggest a possible mitigation strategy.

Pearson — Small companies either stay small, or can grow very quickly into large companies. There is no incentive to be medium sized.

Sowa — While this trend is really more of an economic and national security issue, it does have significant ramifications in cyberspace. For example, what would happen to vulnerabilities if Microsoft were bought by Russian or Chinese Billionaires and moved to Russia, China, or even Iran where they could get educated cheaper labor. Microsoft already does a majority of its software work offshore in India, Pakistan, and other Asian countries. Mid-sized suppliers of Microsoft, Google, and Apple likewise are often based in less-friendly countries.

TERRORISM TRENDS

54. Militant Islam continues to spread and gain power.

It has been clear for years that the Muslim lands face severe problems with religious extremists dedicated to advancing their political, social, and doctrinal views by any

means necessary. Most of the Muslim lands are overcrowded and short of resources. Many are poor, save for the oil-rich states of the Middle East. Most have large populations of young men, often unemployed, who are frequently attracted to violent extremist movements. During its proxy war with the Soviet Union in Afghanistan, the United States massively fortified the Muslim extremist infrastructure by supplying it with money, arms, and, above all, training. It is making a similar mistake today. The overthrow of Saddam Hussein and the American occupation of Iraq has inspired a new generation of jihadis, who have been trained and battle-hardened in the growing insurgency. In a now-declassified National Security Estimate, the American intelligence community concluded that Al Qaeda was more powerful in 2007 than it had been before the so-called "war on terror" began—more dangerous even than it had been when it planned the attacks of September 11, 2001.

Assessment: This trend may wax and wane, but it seems unlikely to disappear this side of a Muslim reformation comparable to those that transformed Christianity and Judaism.

Implications: Virtually all of the Muslim lands face an uncertain, and possibly bleak, future of political instability and growing violence. The exceptions are the oil states, where money can still buy relative peace, at least for now. These problems often have spilled over into the rest of the world. They will do so again.

In a 1994 terrorism study for the Department of Defense and other government clients, Forecasting International predicted that by 2020 a strong majority of the world's 25 or so most important Muslim lands could be in the hands of extremist religious governments. At the time, only Iran was ruled by such a regime. That forecast still appears sound.

Iraq is likely to become the next fundamentalist Muslim regime. Once American forces leave, Iran will support the establishment of a Shiite regime much like its own in Baghdad. There is a one-in-ten chance that this will set off a general war in the Middle East, as Sunni-dominated states intercede to protect Iraqi Sunnis against Shi'a domination. However, Iraq and Saudi Arabia already are negotiating to keep this situation under control.

Any attempt to reduce the commitment of Western forces to the task of stabilizing Afghanistan will result in the restoration of the Taliban to power.

Implications for Information Warfare and Operations: This is one more category of attack that Muslim radicals could mount against their chosen enemies in the West.

One likely source of such an attack would be India, a land with a substantial Muslim minority, about 150 million people, and strong computer and communications industries.

Probability is 85 percent; impact is medium. However, current trends continue to indicate a preference for high-visibility violence instead of potentially more damaging information attacks. The apparent goal of the recent Mumbai attack was to kill "infidels"

and destroy the city's tourist trade. Destroying the telecommunications and power grids would have had much more lasting economic impact.

Expert Comments:

Ayers — It has long been noted that radical Islamists have been using the internet to preach, recruit, glorify suicide-bombers, and perform training on a global basis (see the Intelligence and Terrorism Information Center at the Center for Special Studies publication "*Terrorism and Internet: an examination of Hamas's websites and the hosting providers used by them*" [20 June 2006] and LTG Keith B. Alexander's "Warfighting in Cyberspace," *Joint Forces Quarterly, Vol 43*[3], [2007].) The "e-possibilities" for Islamic militants are obviously limited only to the imagination, just as they are for more harmonious or legitimate activities.

The ability to exploit global media outlets using capabilities provided by digital technology and internet communications is only one aspect. Fraudulent reporting and "doctored" photography utilized by conventional providers (see Richard North, *The Corruption of the Media*, a report published on eureferendum.com [23 August 2006]) have, for instance, swayed public opinion and caused leaders of major nation-states to react in ways that could be seen as generally beneficial to the terrorists' objectives. Similarly, video releases and Internet postings of announcements made by leaders of groups or state-sponsors of terrorism are useful for "global spin"—either by causing a desired reaction or by confusing and thus delaying reactions to specific issues. It should be understood that such announcements may also be part of a duty or a doctrinal requirement (see Stephen Coughlin's *"To Our Great Detriment": Ignoring What Extremists Say About Jihad* [2007]), made much easier by the global nature of the cyber domain.

According to the Islamic equivalent of "Just War" doctrine (see John Kelsay's *Arguing the Just War in Islam* [2007] and *Islam and War: A Study in Comparative Ethics* [1993]), the ruler or rulers of a potential infidel enemy must be provided with an invitation to convert to Islam. Such an invitation, offered by one or more Islamic entities of appropriate (or, in regard to recent cases, remotely appropriate) status and delivered via means of Internet postings to include "virtual worlds" (e.g., "Second Life"), could be considered a chilling new aspect of cyberwar ("new" is used loosely, as this has already been done by Adam Gadahn [see Beila Rabinowitz, "What Al Qaeda's Call for Pipes, Spencer, Emerson, and Scheur to Convert to Islam Means," *Militant Islam Monitor,* 19 September 2006) and via the press by Abu Bakar Bashir [see Irwan Firdaus, "Cleric calls on Bush to convert to Islam," *Associated Press*, 15 June 2006] among others.) The "invitation" is either issued simultaneous with or prior to "a declaration of the resolve of the Muslims to fight, should the enemy refuse" (Kelsay, 1993, p. 35.)

How or *if* a response should be provided, and who should ultimately be held accountable for the wording of any response as well as the consequences thereof, are issues that need very careful consideration. If, however, the invitation is made publically and globally via any sort of new media, the speed of subsequent developments could

be greatly accelerated (as compared to a much slower process such as that seen in the deliberation surrounding several "invitational" letters delivered to world leaders by emissaries of Iran's President Ahmadinejad), necessitating quick reaction to counter potential threat.

A non- or negative response could easily be interpreted as "just cause" for an Islamic "just war"—and in the case of militant Islam, it would be seen as further justification for the global jihad. Cyber warriors on either side of the issue could quickly and easily complicate matters. A traditional response to any invitation to convert would be outright rejection of the opportunity or "accept[ance of] Islam in one of two ways: either they [the invitees] must become Muslims or they must agree to pay tribute as an acknowledgment of the authority of the Islamic state" (Kelsay, 1993, p. 35.) A ruling infidel receiving such an invitation holds the fate of the nation or kingdom in his or her hands when making the decision to either submit to Islam (by conversion or tribute) or pay for the rejection with death (war.) If the ruler rejects the opportunity to submit, the entire nation pays for that decision (Kelsay, 1993.)

University of Gottingen Professor of International Relations and Harvard Research Associate Bassam Tibi described the Islamic "just war" concept as a "Qur'anic command to spread Islam as a way to peace" (See Bassam Tibi's "War and peace in Islam," in T. Nardin [Ed.], *The Ethics of War and Peace: Religious and Secular Perspectives* [Vol 1, pp. 128-145]. Princeton, NJ: Princeton University Press [1996], p. 130.) At this point, it should be mentioned that "peace"—when used by Islamists—is associated with the period of time in which the world is united under the banner of Islam, and is closely associated with "justice," which is believed to exist only under Islamic law (Kelsay, 1993, p. 30; Tibi, 1996.) War should be used as "a last resort in following the basic Qur'anic precept to *guarantee* [italics added] the spread of Islam, usually when non-Muslims hinder the effort to do so" (Tibi, 1996, p. 131.) The cyberworld offers a wealth of opportunity to engage in the spread of Islam, followed by or in conjunction with a cyberwar that would be seen as "just" in the Islamic tradition.

Coates — The information technology aspects of terrorism, small wars, civil wars, and rebellious activity must be thought through afresh, with the primary goal to be winning over people and making them secure in their own terms.

We must develop a policy which throws disruptive events into a realistic framework for effective public policy. The failure to do that, with 9/11, has evoked a response out of all proportion to the losses. IW managers must be prepared to give public guidance to what are small to mid-scale terrorist events like 9/11. Contingency plans of an unfamiliar sort should play a larger and fresh role in military and public policy planning.

Forster — Technology proliferation & communication technologies are facilitating the recruitment, indoctrination, funding, training, and operationalization of terror groups worldwide. As has been known for some time, Al Qaeda is no longer a centrally controlled organization but a networked organization. Information technologies have improved its internal security while permitting cells to coalesce only at the time of attack.

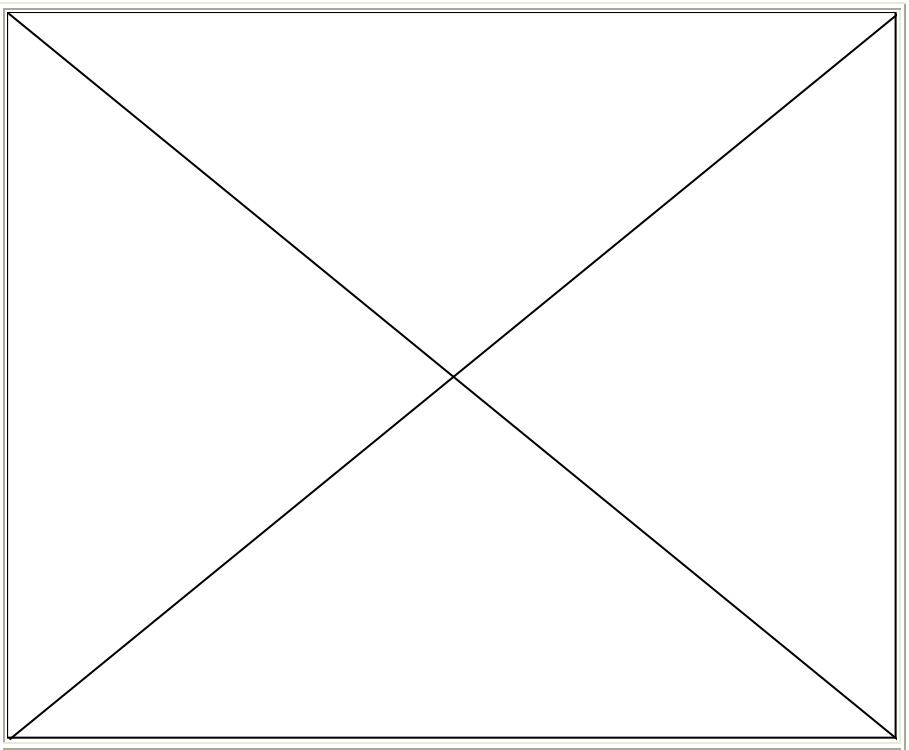
Developments in IT have permitted greater exchange of information while reducing the likelihood of discovery. However, on the positive side, terrorist groups also are more dependent on technology; therefore, successful attacks on their technology infrastructure do more to disrupt planning and execution.

Hoffman — I don't concur with expanding or growing influence of Islamic extremists. These are near term conditions, and an equally valid historical argument for religious extremists and terrorist groups to burn out. See the literature on Audrey Cronin regarding the shelf life of terrorist [movements.]

Leffler—The author respectfully disagrees with assessment that militant Islam will continue to spread and gain power. He predicts that it will peak soon and other extremist-related violence will start to decline globally. He bases this assertion on the rising receptivity of Islamic countries, as well as other countries in the East, to consider Invincible Defense Technology (IDT) as a scientifically verified means to reduce extremism. As evidence, he cites numerous published articles on the topic in the following outlets: *Aljazeera Magazine*, *Arab News*, *Muslim World Today*, *Beirut-Online*, *Muslim*, *Middle East Online*, *Pakistan Daily*, *The Bottom Line*, *The Pakistani Spectator*, *Congo Forum*, *Sri Lanka Guardian*, *The Seoul Times*, *PakTribune, Soldier of Africa, Frontier India Strategic & Defense, Sentinel Review, Congo Watch, India Defence Consultants, Senegambia News, Fiji Daily Post, News From Bangladesh, United News Network, News Wing, MEPeace, Southern Asian Outlook, Northern News Lines, Sudan Watch, Blitz, The Earth Times, Indian Armed Forces, Defence India, Indian Strategic Review, The Tribune, India Defence Consultants, The Daily Excelsior, Defence Talk, Security and Political Risk Analysis Bulletin, Newstrack India, Uganda Watch, New Age Islam, The Morung Express*, and *Islam And Muslims*. Links to these articles and others world wide are available online at: http://www.davidleffler.com/worldwide.html.

Almost all of these above-mentioned publications refer to research in the Middle East, published in the *Journal of Conflict Resolution.* The peer-reviewed research demonstrated that a sufficiently large group of Invincible Defense Technology (IDT) experts in Israel affected the war in nearby Lebanon. The Lebanon War intensity dropped 45 percent, war deaths dropped 76 percent, and quality of life improved by 0.75 standard deviation units. In Israel, crime dropped by 12 percent and quality of life improved by 1.3 standard deviation units. On the same days, a composite quality-of-life index showed decreased crime, traffic accidents and fires in Jerusalem, and decreased crime accompanied by improvements in the stock market and national mood throughout Israel. Other possible causes (weather, weekends, holidays, etc.) were statistically controlled for and could not account for the results. A follow-up day-by-day study in *Journal of Social Behavior and Personality* of more than two years showed that during seven different coherence-creating assemblies, war deaths in Lebanon decreased by an average of 71%. Based on this research and other studies, it is clear that Invincible Defense Technology is capable of greatly reducing protracted sectarian violence.

IDT Group Size and Quality of Life in Israel



Quality of life in Israel improved and intensity of the conflict in Lebanon decreased in direct proportion to the number of Invincible Defense Technology experts in the coherence-creating group (*Journal of Conflict Resolution*, 1988, vol. 32, #4, pp. 776-812). Online video (5:38) featuring Dr. Hagelin explains this finding

It is likely that the militaries of Islamic countries will soon begin using Invincible Defense Technology. When they do, violent tendencies will dissipate. Even if this prediction should not come to pass, one of India's leading antiterrorism experts, Major General (Retd.) Kulwant Singh, Ph.D., and associates are creating a group of 15,000 experts in Invincible Defense Technology (IDT) in central India. Based on the results of peer-reviewed scientific research published in the *Journal of Offender Rehabilitation*, this group should be large enough to reduce terrorism globally. This research showed that deaths due to international terrorism dropped 72 percent and international conflict dropped 32 percent when large groups of experts in IDT were in place. Therefore, when the group of IDT experts in India is large enough, the incidence of terrorist attacks worldwide is predicted to decrease.

(For more information about IDT, see "Utilizing Powerful Peace-Creating Technologies to Combat Cyber Warfare" in Appendix A: "Further Comments from Our Panel of Experts.") [**Editors note**: This Appendix was expanded and featured in the September 2009 *American Heroes Press Newsletter* and it is now available online at *Military Writers*.]

Pearson — Yes, and counter attacks are likely from populations sick of being targeted by Islamists. But lots of new threats will arise from all the other tensions brewing in society. As they see power being wielded successfully by others, they will be more tempted and more able to follow suit.

Rowlatt — Many of the possible scenarios in this paper are simply too logistically heavy for a terrorist to undertake. The terrorist will simply grab and adapt technology and materials on the run. Principally because they want to ensure they leave the smallest footprint possible before and after the attack. Look at the use of cell phones and roadside bombs. We need to look at technology in terms of "adaptive technology", and place technology on a spectrum of adaptability. In this regard, we then redefine smart technology as that technology which has the greatest level of adaptation not the biggest bang.

Sowa — Cyber-attacks by perpetrators will persist. Some portion of the perps will be terrorists that don't care if the mission is suicidal. Some of the more radical examples of possible attacks have already been discussed.

Thomas — Internet ability to cyber mobilize: Internet can train, finance, recruit, etc.

55. International exposure includes a growing risk of terrorist attack.

Terrorism has continued to grow around the world as the Iraq war proceeds, even as the rate of violence in Iraq itself has, at least temporarily, declined. State-sponsored terrorism has nearly vanished, as tougher sanctions have made it more trouble than it was worth. However, nothing will prevent small, local political organizations and special-interest groups from using terror to promote their causes. These organizations have found inspiration in the successes of Al Qaeda, and many have found common cause. The most dangerous terrorist groups are no longer motivated primarily by specific political goals, but by generalized, virulent hatred based on religion and culture.

On balance, the amount of terrorist activity in the world will continue to rise, not decline, in the next 10 years. This was seen in corrections to the State Department's April 2004 report on terrorism, which originally seemed to show a sharp drop in terrorist incidents. In fact, terrorist attacks had risen sharply since the invasion of Iraq, both in number and in severity.

Assessment: This trend is unlikely to change in the next decade and relatively unlikely to change in the next 20 years. A permanent end to the international terrorist threat would require a broad philosophical and cultural change in Islam that makes terrorists pariahs in their own communities. No such change is on the horizon.

Implications: Terrorism against the West is likely to grow, not decline, when fighters trained and blooded in the Iraq war are able to turn their attention elsewhere.

Western corporations may have to devote more of their resources to self-defense, while accepting smaller than-expected profits from operations in the developing countries.

Like the attacks on the World Trade Center and Pentagon, the American embassies in Kenya and Tanzania before them, and the bombings of the Madrid rail system and London subways since then, any attacks on major corporate facilities will be designed for maximum destruction and casualties. Bloodshed for its own sake has become a characteristic of modern terrorism.

Where terrorism is most common, countries will find it difficult to attract foreign investment, no matter how attractive their resources.

Though Islamic terrorists form only a tiny part of the Muslim community, they have a large potential for disruption throughout the region from Turkey to the Philippines.

The economies of the industrialized nations could be thrown into recession at any time by another terrorist event on the scale of September 11. This is particularly true of the United States. The impact would be greatest if the incident discouraged travel, as the September 11 attacks did.

The U.S. economy is being affected already by American anti-terrorism measures. Since Washington began to photograph incoming travelers and to require more extensive identification from them, tourism to the United States is off by some 30 percent. The number of foreign students coming to American universities has declined by a similar amount.

Implications for Information Warfare and Operations: Until the terrorist problem is brought under control—probably not for at least a generation—we will face a growing threat that Muslim extremists will master computer and Internet technologies and use their skills to disrupt essential communications and data. The impact will be seen in American corporations, research laboratories, universities, utilities companies, and manufacturing. Cyber operations will be at best second choices for many terrorists, who prefer newsworthy gore of attacks with bombs and firearms. However, their potential for maximum economic impact with minimum risk eventually will make them irresistible to forward-looking extremists.

Probability is 85 percent; impact is high. Despite their general preference for dramatic bloodshed, noted in Trend 54, we believe that the most professional terrorists eventually will wean themselves away from physical attacks and begin to focus on information attacks. This new style of terrorism will not be nearly as “photogenic,” but ultimately it will be much more effective.

Expert Comments:

Ayers — As evidenced from previous attacks, Osama Bin Laden probably sees the vulnerabilities of his enemies through the eyes of experience associated with civil

engineering (whether that experience was obtained from the family business, from later education, or both.) Given that perspective, he could expect certain limits to the amount of physical destruction and obtain an estimated range of casualties associated with planned acts of terrorism. Those involved in pre-attack surveillance and planning for kinetic operations, as well as those actually perpetrating attacks, would always run the risk of exposing themselves, their leaders, and the nature of their activities to local and international authorities on a physical basis—thus increasing opportunities for disruption at many points and many levels throughout each stage of an attack scenario.

Bin Laden's cyber equivalent will undoubtedly view vulnerabilities—and the potential for destruction –quite differently. The cyber attacker sees the enemy as an object to prod and probe with little (if any) fear of capture and containment. The result of being noticed prior to an assault may simply be the addition of data security measures that may or may not be effective—certainly not as "show-stopping" or potentially deadly as a ramp-up of physical security to a targeted facility. Cyber security measures are merely a series of obstacles to be overcome. They usually require more effort, to be sure; but the global nature of the internet, the ubiquitous availability of data resources and target information, the standardization of software and methods of data manipulation, as well as a limiting of linguistically-imposed boundaries, make target penetration, surveillance, and attack an inviting challenge. Besides, the effects achieved may be well-worth any extra effort extended—especially if the entire operation can be performed from a safe location thousands of miles from the target. A relatively small effort may produce wide-scale damage to enemy infrastructure and possibly even result in casualties.

The cyber attacker may be a lone actor (e.g. single hacker); a member of a group of hackers either operating with criminal intent (e.g. bank robbery) or as a business (contracting their work out for intelligence, military, terror, or vengeance operations); or the attacker could be a member of a terrorist organization—perhaps even a coalition of terrorists, state sponsors, and criminal elements. In fact, the Internet has facilitated the cooperation of "groups with grudges" (large and small), and in-so-doing, enhanced the ability for each group to capitalize on their own strengths—ultimately becoming part of (through a loose affiliation) a bigger, more aggressively confrontational, and more capable entity.

The cyber attacker may or may not be aware of the DIME (Diplomatic, Information, Military, and Economic elements) model of conflict, but nevertheless understands that a nation without information and/or communications will falter economically and (depending on the intent and expanse of attack) militarily. The target may be small numbers of computers or the information and communication assets of entire nation-states. With the use of cyberspace, the timing needed for mobilization and deployment of resources, support groups, team (or cell) members, or military troops is reduced from months (if not years) to days—and possibly hours.

Cyber terrorists can use methods to hide their activities that are extremely difficult for law-laden Western counterterrorism experts to locate. Assimilation into virtual worlds as a wide variety of fantasyland characters or animals is disconcerting enough (see Chris

Vallance, "US seeks terrorists in web worlds," BBC News, [3 March 2008] and Natalie O'Brien's "Terrorists practice on cyber game," *The Australian* [31 July 2007]), but the use of child pornography to pass coded messages is even more disturbing (see Richard Kerbaj, Dominic Kennedy, Richard Owen and Graham Keeley's "Dangerous and depraved: paedophiles unite with terrorists online," *The London Times*, [17 October 2008].) If you add the vast array of social networking sites (e.g. YouTube, Facebook, and a multitude of blogs), you have a very big problem.

Regardless, cyberwar attack modes have already been tested (for the attack on Estonia see Rhys Blakely's and Jonathan Richards' report "UK headed for cyber 'cold war'," *The London Times*, [29 November 2007]; or Mark Landler & John Markoff's "Digital Fears Emerge After Data Siege in Estonia," *The New York Times* [29 May 2007]; and for the Georgia cyber operation see John Markoff's "Cyberspace Barrage Preceded Russian Invasion of Georgia," *The New York Times* [13 August 2008].) There seems to be little doubt that the worst is yet to come.

Forster — Cyber capabilities mean an increase in attacks both from terrorist organizations and individuals who have access to a computer and the "know how" to hack into systems. The increases in vulnerabilities mean additional resources need to be spent on protection and mitigation.

Hoffman — Concur with Frank Sowa on the persistence and adaptation of attacks. Our increasing urbanization and concentration of resources increases our vulnerability, leading to attempts to conduct "systems disruption" attacks per the Open Source Warfare construct of John Robb.

Leffler — Major General (Ret.) Kulwant Singh, Ph.D., and associates are creating a group of 15,000 experts in Invincible Defense Technology (IDT) in central India. Based on the results of peer-reviewed scientific research published in *Journal of Offender Rehabilitation*, this group should be sufficiently large to reduce terrorism globally. This research showed that international conflict dropped 32 percent and deaths due to international terrorism dropped 72 percent when a large enough group of experts in IDT was in place. Therefore, when the group of IDT experts in India is large enough, the incidence of terrorist attacks world-wide is predicted to decrease.

(For more information about IDT see "Utilizing Powerful Peace-Creating Technologies to Combat Cyber Warfare" in Appendix A: "Further Comments from Our Panel of Experts.") [**Editors note**: This Appendix was expanded and featured in the September 2009 *American Heroes Press Newsletter* and it is now available online at *Military Writers*.]

Pearson — Of course, but staying within a country still leaves you open to home grown threats, and international migration mixes all the people up so that tribal threats are everywhere anyway.

Rowlatt — National security needs to address the freedom big business has in moving its IT services off shore. If a business is a major contributor to a nation's GDP, then what right does it have to expose its Cyber Underbelly, to a foreign power, which in turn, exposes the nation to unnecessary cyber risks? Look at how terrorists targeted Mumbai which is the cyber centre for India, which serviced many international organizations IT needs.

Sowa — Cyber-attacks by perpetrators will persist. Some portion of the perps will be terrorists. The attacks should move over the next 20 years from solely physical attacks to combination cyber- and physical-attacks to a focus of cyber-attacks as stated to a complex attack designed to carry out a specific mission toward a greater end (similar to U.S. shock and awe strategic planning when we attacked Saddam Hussein—on a dramatic, but much smaller scale—i.e. oil refineries, nuclear plants, chemical plants, harbors, subways, entertainment facilities, hospitality and restaurant facilities, financial facilities; or Mumbai-style attacks).

CONCLUSION

Last November, the National Intelligence Council's report *Global Trends 2025: A Transformed World* forecast, "Conflict will continue to evolve over the next 20 years as potential combatants adapt to advances in science and technology, improving weapon capabilities, and changes in the security environment."

Building on this insight, that study identified a number of strategic trends that the authors believed would change the nature of warfare over the next 15 years. For our present purpose, one stands out:

The Increasing Importance of Information. "Advances in information technologies are enabling new warfighting synergies through combinations of advanced precision weaponry, improving target and surveillance capabilities, enhanced command and control, and the expanding use of artificial intelligence and robotics. … The growing importance of information technologies as an enabler of modern warfighting capabilities will make information itself a primary target in future conflicts. By 2025 some states probably will deploy weapons designed to destroy or disable information, sensor, and communication networks and systems…."

In a talk that anticipated publication of *Global Trends 2025*, deputy director Thomas Fingar, of the Office of the Director of National Intelligence, took this a step further. He suggested that American nuclear power will become less important as challenges shift to cyberspace.

In this, he was correct. Our major concern is no longer weapons of mass destruction, but weapons of mass disruption. The cost of "going nuclear" is simply too high for atomic weapons to be used by any but a rogue state unconcerned with its own survival. Cyberweapons may kill fewer people, but they can have enormous economic impact. A particularly clever opponent might even carry out a devastating attack without ever

being identified or facing retribution. Information has become the battlefield of choice. It will remain so well into the future.

This is a lesson that many of America's potential antagonists clearly have taken to heart. The U.S. Government Printing Office reports that *Global Trends 2025* was its best-selling publication in 2008, quickly exhausting several large print runs. Three-fourths of the copies went to readers in other countries.

The present study offers several more insights about cyberwar and the future of American security:

As the world becomes more dependent on information technology, it becomes more fragile. It is possible to make any specific site or network more secure, but not the "system" as a whole. As network connections proliferate, electronic controls—for example, of petroleum refineries, chemical plants, or electrical grids—become more complex and interlinked, and the number of users grows, the opportunities to interfere with its operations expand exponentially. There is a growing possibility that even accidental missteps could cause significant harm. This damage would not necessarily be limited to data but could strike at real-world infrastructure, with potentially devastating effects. Economic losses could be severe, and loss of life is possible.

Cybercrime could be as significant as cyberwar. Four members of our panel cited profit-motive information crimes as a problem of potential importance. An information "protection racket" aimed at financial institutions could entail serious economic risks, and perhaps security risks as well. These crimes might use many of the same techniques as information warfare and could be difficult to distinguish from it. Indeed, in a world where rogue governments have supported themselves in part through counterfeiting major currencies, there may be no useful distinction. However, it is not clear that cyberwar and cybercrime will be amenable to the same countermeasures.

The rise of artificial intelligence (AI) will change the nature of cyberwar. As computer systems "learn" to imitate human reasoning and skills, The nature of cyberwar will change. Instead of relying on human hackers to carry out their attacks, antagonists will automate their information warfare, relying on AI systems to probe opposing defenses, carry out attacks, and defend against enemy AI. This competition will quickly outstrip human control, or even monitoring. This is one aspect of the hypothetical "singularity," the time when artificial intelligence exceeds our own and it becomes impossible even in theory to predict what will happen in the further future.

The United States is losing its leadership in critical technologies. As other countries build up their technological capacity, the U.S. is allowing its own to deteriorate. As China and India turn out more scientists, engineers, doctors, and technicians, the United States has been producing fewer. As other lands spend more on research and development, the U.S. has been spending less. And as other countries devote more of their research budgets to fundamental science, where breakthroughs happen, the U.S.

has focused increasingly on short-term applications. All this may put America at a serious disadvantage in future cyberwars.

Each of these issues will have a significant impact on American cyber-security in the years ahead. Each merits detailed study.

Recommendation

While this study has produced some valuable results, it clearly is no more than a preliminary work. Many questions remain to be resolved about the nature and impact of future information warfare. What are our most likely targets for attack? What tactics will our adversaries use? How can we best defend against them? These are material for a follow-on study, and we recommend strongly that it be undertaken as quickly as possible. The United States cannot devise a rational strategy to defend against cyber attack until the questions above, and many others, have been answered.

Whether Forecasting International pursues this research or another organization takes it on, we also recommend that the study employ an expert panel of intelligence specialists, military thinkers, and general forecasters. We first employed this combination of skill sets when managing the Fourth Annual Defense Worldwide Combatting Terrorism Conference in 1994. Our report from that meeting, *Terror 2000: The Future Face of Terror*, correctly anticipated virtually every aspect of terrorism as it has unfolded in the years since then, from the rise of Muslim extremism as a source of international attacks to the deliberate crash of an airplane into the Pentagon. We attribute this success to the power of uniting the diverse experience and skills of intelligence, military, and forecasting professionals to answer difficult questions. We have employed that combination with great success on many occasions over the last 15 years.

We further recommend that any future study draw on many of the same people employed in the current work. These “best of the best” have proved to be extremely insightful, creative, and dedicated to improving the security of the United States and its allies. These people include:

Intelligence: “Anonymous, Senior Intelligence Officer, Joint Staff Directorate for Intelligence, J2;” Cynthia E. Ayers, John C. Coale, Bahukutumbi Raman.

Military: “Anonymous, senior researcher at a Beltway think tank;” Dr. Jonathan Czarnecki; Francis G. Hoffman.

Forecasting: Joseph Coates, Ian Pearson, John L. Petersen, John W. Peterson, David Pearce Snyder, Frank Sowa, Dr. Stephen F. Steele.

Participants’ Biographies

We wish to thank the following people for their enormous contributions to this work. If there is value in this report, much of the credit goes to them.

We particularly offer our gratitude to Frank Sowa, one of the most capable forecasters now practicing. His labors on our behalf went far beyond any possible call of duty.

Anonymous

Senior researcher at a “Beltway” think tank.

Anonymous, Senior Intelligence Officer, Joint Staff Directorate for Intelligence, J2

Little more to be said!

Anonymous source at the UK Ministry of Defence

Two individuals.

John Auger

John Auger, a retired military officer, is a senior analyst supporting Proteus USA and also serves as the program manager for Booz Allen Hamilton at the United States Army War College.

Cynthia E. Ayers

Prof. Ayers is NSA Visiting Professor of Information Superiority, Center for Strategic Leadership, U.S. Army War College. She has worked within the intelligence community for over 35 years. Her most recent assignment prior to her arrival at the U.S. Army War College was as a National Security Agency Representative to the DCI’s Counterterrorism Center (2000-2002.) In her current position, she teaches senior officers of all U.S. military services (reserve and active duty) as well as allied officers from foreign services. Prof. Ayers has authored and coauthored several papers on national security topics, considering issues of religion, culture, and conflict.

Mark Callanan

Dr. Mark Callanan is a lecturer and public policy specialist with the Institute of Public Administration in Dublin. Before joining the Institute, Mark worked with Deloitte & Touche in Brussels. He is responsible for providing a range of services to central government and local authorities in Ireland, has undertaken commissioned research for a range of government agencies and the European Commission, has spoken at domestic and international conferences, and provided training courses for public servants in 12 European countries.

Mark is project manager for a futures project on the Irish public service. This project is examining global and national trends and drivers of change within the public services over the coming years. This involves analysing some of the challenges for public

service providers on the horizon, and assessing how ready the public service is to cope with different eventualities. Ultimately, the project is aimed at provoking thinking about long-term trends, including demographic, societal, economic, technological, environmental, and workplace trends, and how these may impact on public service provision. These are being used to consider the state of readiness of the public sector to meet some of the different challenges ahead, with a view to identifying choices and changes that are needed in the light of emerging trends.

Mark is also a member of the high-level Local Government Customer Service Group, set up by the Irish Minister for the Environment, Heritage and Local Government, containing representatives from central government, local councillors, county and city managers, directors of service, to examine a number of issues related to local government, including performance indicators, corporate planning, customer surveys and complaints and redress systems. Part of my contribution to the Group has involved undertaking research into best practice in both Ireland and abroad in these areas.

Mark obtained a PhD in Commerce from University College Cork, Ireland, and a Masters from the College of Europe, Bruges, Belgium.

Dr. Edward J. Cetron

Dr. Cetron is a researcher and data analyst who has frequently worked with Forecasting International on reports to clients in government and industry. His significant activities with FI include research participation in *Terror 2000: The Future Face of Terror*, an extremely successful forecast of terrorist activities in the years since 1994, and a forecast of the possible impact of terrorism on a major American bank. Dr. Cetron holds a doctorate in bioengineering from the University of Utah and degrees in chemistry and physics/computer science from the University of Virginia, Charlottesville.

John C. Coale

As a career government employee, I have over 30 years of government service, including 21 years in the intelligence community. This background, along with my lifelong fascination with history, military strategy, and geopolitics, enabled me to achieve my long-held personal goal of teaching at the college level.

After beginning my career as a civilian electrical engineer with the Navy, I moved on to modeling and simulation of foreign platforms and weapons systems in support of US naval capabilities. I spent ten years at the Defense Intelligence Agency; my work there included all-source senior intelligence analysis and reporting in the areas of advanced telecommunications technologies, information warfare, national and foreign critical infrastructures, computer network operations, modeling and simulation, and foreign naval platforms and weapons. I'm still with the Department of Defense as a technical director.

Major career achievements include Intelligence Community Officer Designation (2002), M.S. degree in Strategic Intelligence from the Joint Military Intelligence College (1996),

US Navy Civilian Meritorious Service Award and Medal (2002), and National Y2K Medal (2000).

Joseph Coates

Joe Coates is one of the most broadly experienced and diversified futurists in the United States. For 25 years he has had his own futures business doing projects and consulting to half of the largest corporations in America, agencies of government at all four levels, and countless trade and professional associations. In addition to his proprietary work, he has published over 300 articles and wrote or co-authored five books. Earlier he was Assistant to the Director for methodology at the now defunct Congressional Office of Technology Assessment. Before that, he was program manager at the National Science Foundation in the program Research Applied to National Needs, with a strong emphasis on anticipating the consequences of new and emerging technological and scientific developments. In the 1960s he spent eight years at the Institute for Defense Analyses, where his special interests were revolutions, small wars, crime, chemical and biological weapons, and non-lethal weapons. His earlier professional career was as a research chemist at a multinational corporation.

Jonathan E. Czarnecki, Ph.D.

Dr. Jonathan Czarnecki teaches joint and interagency operations for the Naval War College at the Naval Postgraduate School in Monterey, California. He is a retired colonel in the United States Army and Army National Guard. He received his Masters and Doctorate in Political Science from the University of Buffalo; his Bachelor of Science is from Clarkson University. Dr. Czarnecki is a certified professional planner, facilitator and quality management consultant. He has published over thirty articles on topics as diverse as military operational art and futures research. Dr. Czarnecki has had a variety of careers including academic professor, military officer, futurist, political analyst, lobbyist, and poet. His current major research and teaching interests concern a development of a deep understanding of the role and meaning of information in warfare and explaining the success or failure of combat operations.

Peter Forster, Ph.D.

Peter Forster is affiliate faculty in the Department of Political Science, Pennsylvania State University, and represents the department and the Social Science Research Institute on NATO's Consortium for Defense Academies and Security Studies Institutes, part of the Partnership for Peace initiative. Although he has participated in a number of the Consortium's activities, he is most active in the Security Sector Reform Working Group. This group's agenda dovetails with his research interest in national security and civil-military relations. Currently, he is pursuing research on civil-military relations in former Soviet Central Asia. He earned a certificate in National Security Studies from Christian-Albrechts University in Kiel in 1989 and received his Ph.D. in International Relations from Penn State in 1997. In addition to national security, he is interested in US Foreign Policy and international relations of the Middle East. Dr. Forster has just

completed a co-authored manuscript on the evolution of burden sharing beyond NATO's traditional area of operation.

Dr. Forster is currently the Associate Director for Academic Programs in Penn State's World Campus. He has used his background in history and international relations to develop new international initiatives at Penn State that include the first distance learning program to be established in Russia outside of St. Petersburg and Moscow. He also has consulted on the development of national distance education programs in Central Asia and presented papers and written on distance education.

Dr. William E. Halal

Bill Halal is Professor Emeritus of Science, Technology, and Innovation at George Washington University and President of TechCast LLC, an online think tank specializing in forecasting developments in technology. His recent book, *Technology's Promise: Expert Knowledge on the Transformation of Business and Society* (Palgrave MacMillan, 2008), provides a wide-ranging and generally optimistic look at where technology will lead the world in the years ahead.

Francis G. Hoffman

Mr. Frank Hoffman is a Research Fellow at the Marine Corps Center for Threats and Opportunities, as well as a nonresident Senior Fellow at the Foreign Policy Research Institute. Mr. Hoffman's career includes 24 years as a Marine infantry officer and several tours at the Pentagon. He has served on the staff of the Commission on Roles and Missions of the Armed Services, and the U.S. National Security Commission/21st Century where he developed the organizational design for the Department of Homeland Security. He also served on three Defense Science Boards. He is a frequent contributor to professional military journals on strategy, homeland security, defense economics and military innovation. His recent contributions include "Dereliction of Duty Redux?, Post-OIF Civil-Military Relations" in the Spring 2008 issue of Orbis. A graduate of the University of Pennsylvania, Mr. Hoffman holds graduate degrees from George Mason University and the Naval War College.

John Kapinos

John Kapinos is veteran of almost thirty years in Law Enforcement. He served a 25-year career with the Montgomery County (MD) Police Department, where his career highlights included serving as the Department's Policy and Planning Director under former Chief Charles Moose, as well as staffing a management role on the D.C. Sniper Task Force in 2002. Since 2005, John has worked as a civilian strategic planner with the Fairfax County (VA) Police Department.

John holds a bachelors degree from the University of Maryland and is a Certified Public Manager through George Washington University. John is a member of the International Association of Chiefs of Police, The Police Executive Research Forum, Police Futurists

International, and the International Association of Law Enforcement Planners (where he served as President in 2006.)

Captain Norman Lewis Kaufman, U.S. Navy (Retired)

Capt. Kaufman is a former merchant mariner, a retired naval officer, and a management consultant. He holds degrees from the U.S. Merchant Marine Academy (1948), the Armed Forces Staff College (1965), and the Industrial College of the Armed Forces (1972), culminating in an MSA, George Washington University (1972) and Graduate Certification (HCA) from George Washington University (1979.) He concluded a 27-year Naval career in 1977 as Commanding Officer of the Human Resource Management Center, Washington DC.

Bruce LaDuke

Bruce LaDuke lives in Greenwood, Indiana with his wife Brenna and four children. He works full-time in a global corporation and has over 20 years of fortune 500 experience in a variety of business roles. For over 25 years, Bruce has engaged in part-time private research in questioning. From a deep understanding of the question, he has evolved a merger of all creative method, a 'process-centric' model for human knowledge working, an advanced knowledge philosophy, an integral futuring method, and a model for artificial knowledge creation that provides a deeper understanding of simultaneous knowledge convergence and singularity. Bruce also partnered with an associate to create SOPAC, a powerful, integral performance system that can be applied in any social, business, or military initiative.

Dr. David R. Leffler

David R. Leffler, Ph.D., is the Executive Director at the Center for Advanced Military Science at the Institute of Science, Technology and Public Policy. He is also the Director of the Division of Enlightened Defense at the Institute for Development of Enlightened Arts and Sciences. He serves on Board of Editors for the *Journal of Management & Social Sciences*. Dr. Leffler received his Ph.D. from The Union Institute & University in Cincinnati, Ohio, where he did his doctoral research on the topic of Invincible Defense Technology. He served in the U.S. Air Force for eight years. He is an Associate of the Proteus Management Group at the Center for Strategic Leadership, US Army War College. His email address is drleffler@hotmail.com. His websites are: www.DavidLeffler.com, www.StrongMilitary.org and www.InvincibleMilitary.org.

Major Matthew Lennox, U.S. Army

Major Lennox is instructor in American Politics, Policy, and Strategy at the U.S. Military Academy at West Point. He commissioned as a Field Artilleryman and has peace enforcement and combat experience in Kosovo and Iraq. Major Lennox holds a master's degree in Information Security Policy and Management from Carnegie Mellon

University and a bachelor's degree in Electronics Engineering Technology from Texas A&M University.

Ian Pearson

Ian Pearson graduated in 1981 in Applied Mathematics and Theoretical Physics from Queens University, Belfast. After four years in Shorts Missile Systems, he joined BT Laboratories as a performance analyst, and later worked in network design, computer evolution, cybernetics, and mobile systems. From 1991 until 2007, he was BT's Futurologist, tracking and predicting new developments throughout information technology, considering both technological and social implications. He now does exactly the same things for Futurizon, a startup futures institute. As a futurologist and consultant, he lectures widely on his futures views. In between conferences, he writes on topics such as machine consciousness, human evolution, women's issues, ageing, social trends, and advanced computing technology.

He has received many awards for his papers, written several books and has made well over 400 TV and radio appearances. He is a Chartered Fellow of the British Computer Society, the World Academy of Art and Science, the Royal Society of Arts, the Institute of Nanotechnology and the World Innovation Foundation. He was recently awarded an Honorary Doctor of Science degree by the University of Westminster.

John L. Petersen

John L. Petersen is founder of the Arlington Institute, a nonprofit, future-oriented think tank and editor of the e-newsletter *FUTURE-dition*. Petersen also is author of *Out of the Blue: How to Anticipate Wild Cards & Big Future Surprises* and *Vision of 2012: Planning for Extraordinary Futures*.

Mr. Petersen is best known for writing and thinking about high impact surprises—wild cards—and the process of surprise anticipation. His current professional involvements include the development of sophisticated tools for anticipatory analysis and surprise anticipation, long-range strategic planning and helping leadership design new approaches for dealing with the future.

Petersen's government and political experience include stints at the National War College, the Institute for National Security Studies, the Office of the Secretary of Defense, and the National Security Council staff at the White House. He was a naval flight officer in the U.S. Navy and Navy Reserve and is a decorated veteran of both the Vietnam and Persian Gulf wars. He has served in senior positions for a number of presidential political campaigns and was an elected delegate to the Democratic National Convention in 1984. His 1988 book-length report "The Diffusion of Power: An Era of Realignment" was used at the highest levels of American government as a basis for strategic planning.

John W. Peterson

John W. Peterson (augmentation10@aol.com) is a retired Bell Labs/Lucent Technologies technology strategy manager. He is currently the managing director of The Strategy Augmentation Group, Inc., and sometimes team-teaches at Northwestern University (NU) as an adjunct. NU participation has included "International Technology Strategy" at the Kellogg Graduate School of Business, "Business Intellectual Property Strategy" at the School of Law, and he serves as an advisory board member to the Master's in Product Design program at the NU McCormick School of Engineering and Science. He has several patents and has served as a member of editorial advisory board of the international journal, *Technological Forecasting and Social Change*. He occasionally provides support to IC futures activities (i.e., National Reconnaissance Office's "Project Proteus," National Imagery and Mapping Agency's "Understanding Global Change;' the National Intelligence Council's "Tech 2020," etc..) He served in Vietnam as a rifle platoon leader and battalion staff officer (3/21st Inf and 6th Psyop.)

Bahukutumbi Raman

Served in the Intelligence Bureau, India's internal intelligence agency, from July 1967 to September 1968 and in the Research & Analysis Wing (R&AW), India's external intelligence agency, from September 1968 to August 1994. Retired in August 1994 as the head of the counter-terrorism division of the R&AW after having served in that capacity for six years. Was a member of the National Security Advisory Board of the Government of India from July 2000 to December 2002. Was a member of a special task force appointed by the Government of India in 2000 for making recommendations for revamping the Indian intelligence community. Was a member of the Working Group on Terrorism of the Council On Security Co-operation Asia Pacific (CSCAP) in 2002 and 2005. Author of four books: *Intelligence—Past, Present & Future* (2001), *A Terrorist State As A Frontline Ally* (2001), *The Kaoboys of R&AW—Down Memory Lane* (2007), and *Terrorism—Yesterday, Today & Tomorrow* (2008). All published by the Lancer Publishers of New Delhi—www.lancerpublishers.com.

LTC Kevin Gary Rowlatt

Lieutenant Colonel Kevin Rowlatt joined the Australian Army in 1984 as a soldier, where he served as an Aircraft Handler with the 1st Aviation Regiment. In 1988, he graduated from the Royal Military College — Duntroon and was commissioned as a Lieutenant in the Royal Australian Engineers.

As a Lieutenant, he held appointments as Troop Commander with the Divisional Engineers and as an Engineer Instructor with the School of Military Engineering. During his time as a Captain, he was fortunate enough to hold both regimental and staff appointments including Corps Adjutant to the Director of Engineers — Army. On promotion to Major, Kevin was responsible for the coordination of Recruit and Initial Employment Training for Training Command — Army, before attending Australian Command and Staff College in 2000. Kevin has spent the last six years in Army Career Management both as a Major and as a Lieutenant Colonel, culminating in the post of

Chief of Staff Career Management — Army. He took up his current appointment as Australian LNO to TRADOC in Dec 06 and has a three-year tenure.

T. Irene Sanders

T. Irene Sanders, executive director of the Washington Center for Complexity and Public Policy, is author of "Strategic Thinking and the New Science: Planning in the Midst of Chaos, Complexity and Change." (The Free Press.)

David Pearce Snyder

David Pearce Snyder is a consulting futurist and a data-based forecaster whose seminars and workshops on strategic thinking have been attended by representatives of most Fortune 500 companies. Mr. Snyder has published hundreds of studies, articles and reports on the future of a wide range of industries, institutions and professions, and on the socio-economic impacts of new technology. He is contributing editor of *The Futurist* magazine. His office is in Bethesda, Maryland, where he can be reached at 301-530-5807; or e-mailed at david@the-futurist.com; his website is www.the-futurist.com.

Frank Sowa

Frank Sowa, IEEE, is CEO of The Xavier Group, Ltd. A strategic planning consultant and futurist, he assists individuals and organizations examine the underlying processes and methods that aid in improving data collection and mining, content analysis, strategic planning, forecasting, and systemic transformation.

A project manager and executive director for the sixth largest engineering and construction firm in the world, Mr. Sowa was an Internet pioneer—working on creating collaboration networks as early as 1979, and having a Fidonet BBS-link system running in 1983. Mr. Sowa is a certified computer developer, a software and database developer, and networking solutions consultant on a number of platforms.

In 1986, he established the 16th commercial Internet Service called "SEED.NET" the "Start-Up Entrepreneurial Economic Development Network" hosted on Carnegie Mellon's Andrew server farm, and as a part of the Internet via PREP.NET.

In 1986, Sowa also invented the Chronometric Modeler, a computer simulator that analyzes how trends are impacted by emergent factors over time. More recently, his work has been involved in the building of inexpensive 3D virtual communities for instructional purposes, and unique and vital communications concepts of collaborating over networks, designing comprehensive web-based content services, and creating e-learning environments.

He has worked with well-known organizations, federal, state, and local government agencies, educational institutions, and non-profits of all sizes who are seeking out smarter ways of using knowledge for strategic advantage.

Mr. Sowa can be reached at fxsowa@gmail.com.

Dr. Stephen F. Steele

Stephen F. Steele is the originator and former director of the Institute for the Future @ Anne Arundel Community College, Arnold, Maryland (www.aacc.edu/future .) He currently serves the college as a professor of sociology and futures studies. Steve has been active and visible in futures work and applied sociology for over three decades. He has been a contributor and a Delphi participant on several projects for Forecast International.

Timothy Thomas

Lieutenant Colonel Timothy L. Thomas, U.S. Army, Retired, is a senior analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He holds a B.S. from the U.S. Military Academy and an M.A. from the University of Southern California.

Patrick Tucker

Patrick Tucker, M.A., is the senior editor of *THE FUTURIST*, an international consumer magazine about social and technological trends. He has been quoted as a futurist and trendwatcher in such publications as *The Chicago Tribune, the Globe and Mail, The Daily Record, The Washington Post, The New York Times online, Elle Canada, The Edmonton Journal, Ottawa Citizen, Saskatoon Star-Phoenix, Vancouver Sun, Calgary Herald, Halifax Daily News, Victoria Times Colonist, Nanaimo Daily News, Winnipeg Free Press, Windsor Star*, Wired.com, *LapTop magazine, PC World,* Discovery.com and Smart Money.com and has been a guest on such radio networks and programs as WTOP in Washington, the Dave Rutherford Show (770 CHQR Canada) The World Today and the Christy Clark show (980 CKNW Canada), the Joan Hamburg show (710 WOR New York), London in the Afternoon (1290 CJBK) SCIENCE FANTASTIC with Michio Kaku and the Discovery Channel. He manages all of the editorial content and consumer programming on the World Future Society site and direct all media outreach for *THE FUTURIST*. Patrick also serves as the director of communications for the World Future Society, publisher of *THE FUTURIST*, a scientific organization based outside of Washington DC.

Nico van Klaveren

Dr Ir Nico van Klaveren has technical science and business degrees from Delft Technical University (The Netherlands) and Pepperdine University.

Taught at Delft and Stevens Institute of Technology.

Worked for Chevron Corporation on applying computer technology for process design and planning,

computer aided education, artificial intelligence and simulation games.

Presently consultant (VanKay Consulting).

Lawrence W. Vogel

Lawrence Vogel is a senior IT and business management consultant to private-sector organizations and headquarters and field elements of federal agencies including the Department of Defense, Department of Energy, Department of State, the former Immigration and Naturalization Service, and the Department of Homeland Security. His major focus is currently on information and business systems related to homeland security including emergency management and customs and immigration enforcement. He has provided business and technology management, technology transfer, and systems engineering assistance to private sector clients in the oil and gas and environmental industries.

Mr. Vogel is a licensed professional engineer with a Bachelors degree in Civil Engineering, a Masters degree in Petroleum Engineering, and a Masters of Business Administration.

Forecasting International Staff

Dr. Marvin J. Cetron

Dr. Cetron is founder and president of Forecasting International. For some 50 years, he has pioneered corporate and government forecasting, developing many of the techniques that other forecasters now use daily. He remains one of the most active and respected practitioners in this field.

During this long and productive career, Dr. Cetron has consulted for more than 400 of the *Fortune* 500 firms; over 100 government agencies, among them the Central Intelligence Agency, the Transportation Security Administration, and the National Security Agency; and 150 professional and academic associations. He served as an advisor to the White House for every administration, Republican and Democratic, from the time of John Kennedy through the Clinton years.

Dr. Cetron's 1994 study, *Terror 2000: The Future Face of Terror*, circulated privately at the Pentagon, predicted virtually the entire course of terrorism in the years since.

Owen Davies

Senior analyst Owen Davies has worked with Forecasting International since 1986. During that period, he has researched and written approximately 100 studies for

government agencies, commercial clients, and professional associations, including the Department of Defense, and the National Security Agency; Best Western, Capital One, Saab-Scania, and Siemens Engineering; and the Society of Surgical Oncology. A prolific author in the fields of medicine, science, technology, and the future, he has written 18 books, many of them with Dr. Cetron; uncounted magazine articles; and many business reports and other specialized works.

Justin Cetron

Research analyst Justin Cetron has been with Forecasting International since 2004. His projects include the report "Terrorism Targets: Analyzing Probabilities and Impacts" and significant contributions to FI's monographs for Proteus USA, a nonprofit publishing house associated with the National Intelligence University. He holds a Master's Degree in Information Technology from the University of Delaware.

Annotated Bibliography

1. Hyun Seok Yoon, et al., "A Study on the Information Superiority of Network Centric Warfare for Future Battlefield," in *Information Science and Security, 2008. ICISS. International Conference on Information Science and Security*, Seoul, 2008, pp. 224-231; ISBN: 978-0-7695-3080-X

Information superiority plays very important role for winning the war. Recent warfield have been shown rapid and precise because of new technology. Technologies such as VoIP, wireless LAN, WiBro, RFID and Bio recognition appear as new technologies for giving and receiving information effectively in our current world, it is believed to take superior position of information to address weaknesses in information transferring and protection for each system and then apply them future battlefield information system. In this study, reviewing future battlefields system that US army goes after and those of Korean army will suggest how to accomplish information superiority for army in future battlefields.

1. Jatinder N. D. Gupta, Sushil K. Sharma, *Handbook of Research on Information Security and Assurance*, Idea Group, Inc., 2008

Even though weapons and money are considered important factors for running a modern world, at the end of the day, it is all about controlling and exploiting information for political, military, economic, and commercial advantage. The objective of this chapter is to present a basic understanding of the concept of Information Warfare (IW) and the need for relevant strategies to aid its successful implementation. IW is an important topic in this electronic era and within enterprises, security strategies, tools, and processes are essential in order to maintain a competitive advantage against an adversary or group of adversaries. In this chapter; a Survival of the Fittest IW (SFIW) conceptual framework is presented based on the adaptive nature of IW, and a case study is used to discuss its validity.

1. Olen L. Kelley, "Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative," Army War College, Carlisle Barracks, PA (2008)

In 2001, Joint Publication (JP) 3-0 identified five warfighting domains. The document contained the commonly accepted four operational environments, but added a new domain: "information." This landmark inclusion started an intense debate within the Joint community. Previous clarity on the commonly accepted operational environment's roles and functions became blurred. Those who advocated information as a warfighting domain advanced its common understanding, yet could not reach doctrinal consensus. Discussions about how to describe, organize, and use the United States' information capabilities to support the Department of Defense's (DoD) strategic and operational objectives and national security goals remain contentious and ambiguous. This inability to develop consensus led to the re-characterization of information in the current JP 3-0, "Joint Operations," from a warfighting domain to an "environment." However, this change did not resolve the fundamental issue and the information domain debate continues unabated. The recently published "National Military Strategy for Cyberspace Operations" (NMS-CO) again officially codified its understanding of "information," now defined as cyberspace, as a warfighting domain. It acknowledges the JP 3-0 information domain change to environment, but emphasizes that "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations." The DoD has expended considerable effort in a "piece meal" strategy that updates information-related doctrine based on new technology instead of developing a comprehensive cyberspace strategy. This paper argues that a clear consensus is needed to establish a "cyberspace domain" where JFCs conduct war "as an act of force to compel our enemy to do our will." Advancing the proposed NMS-CO's cyberspace domain definition clarifies information operation's roles and functions, thereby enabling information superiority.

1. Roca, MAJ Raimundo Rodríguez, "Information Operations during Counterinsurgency, Operations: Essential Option for a Limited Response"

The importance of Information in the XXI century has become a fact that nobody can deny.

The relevant role of the Information in societies can be observed as well during the development of conflicts where western forces participate. That is one of the reasons why controlling information flow arises as a significant requirement.

The purpose of this article is to present a theory of operational and tactical information operations (IO) employment, as limited and non-lethal effects during counterinsurgency operations (COIN), with an important role to support area control. Firstly, this study will mainly focus on four integrating elements of IO: psychological operations (PSYOPS), civil-military operations (CMO), public affairs (PA) and computer network operations (CNO.) Secondly, a practical case of IO execution will be simulated and a concept of operation will be developed.

It should be noted that the approach presented herein is from a Spanish Army perspective. As we will appreciate in this article, the knowledge and managing of IO and the employment of CNO as a tool to empower PSYOPS, CMO and PA activities is of extreme significance and it will become essential to understand and to face the scenes of future conflicts and new wars.

1. Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?"

Comparative Strategy 27(3) May 2008 pp. 227 — 247

In April-May 2007, Estonia experienced several weeks of coordinated cyberattacks against its financial and sociopolitical institutions. Although the origin of these attacks cannot be definitively named, it is widely believed in Estonia and among many analysts that Moscow was behind these attacks. Certainly these attacks represented the culmination of plans set in motion a year earlier to attack the Estonian government and society for their supposedly anti-Russian policies. And the accompanying demonstrations in Tallinn at this time also represented well-worn Soviet techniques used in earlier coups in Eastern Europe. Ultimately the advent of such new forms of military operations confirms a threat assessment by which any one operation on land, sea, air, underwater, or space can target anyone in any of these dimensions and raises provocative issues for both analysts of war and government officials.

1. Al-Rizzo, Hasan M. "The Undeclared Cyberspace War Between Hezbollah and Israel" *Contemporary Arab Affairs* 1(3) July 2008 pp. 391 — 405

The self-explanatory title of this article adds a new dimension to the regional conflict. The use of cyberspace warfare in the Middle East is a topic that has been rarely addressed and the article provides interesting insights into various aspects and developments in this new type of conflict.

1. **Stringer, Rob. "**War in the Wires" ***Infosecurity***5(6) September 2008 p. 10

The conflict over South Ossetia has invited a series of cyber-attacks and spam. **Rob Stringer** sorts through the political propaganda and the less sinister opportunist attacks closer to home.

1. Devine, Jack "Tomorrow's Spygames" *World Policy Journal* 25(3) Fall 2008, pp. 141-151

1. "Intel Director: Iran, Cyber Threats biggest worry"

   Associated Press, Friday, January 16th, 2009.

AP talks to Intelligence Director Michael McConnell, who says "Cyber security is the soft underbelly of this country." He recommends that the federal government build a much

more rigorous cyber protection plan, and to integrate the key spy agencies like the NSA into the loop is critical.

1. Bruno, Greg. "The Evolution of Cyber Warfare" February 27th, 2008

The author of this article looks into cyber warfare as coming to be more of an offensive weapon vs. a defensive one, also saying that while the capabilities of the United States aren't known, some of the capabilities can be guessed at. Also goes into brief discussion about spyware and malware. "Less common but far more worrisome are cyber attacks aimed at critical infrastructure—like nuclear-power-plant control systems, banks, or subways. In March 2007, the Department of Energy's Idaho Lab conducted an experiment to determine whether a power plant could be compromised by hacking alone. The result—a smoking, self-combusting diesel generator incapacitated by nothing more than keystrokes—sent shivers (CNN) through the private sector. The worries were apparently well-founded. In January 2008, a CIA analyst told U.S. utilities that hackers had succeeded in infiltrating electric companies in undisclosed locations outside the United States and, it at least one instance, shut off power to multiple cities."

1. *Global Trends 2025: A Transformed World*, National Intelligence Council, November 20th, 2008.

Global Trends 2025: A Transformed World is the fourth unclassified report prepared by the National Intelligence Council (NIC) in recent years that takes a long-term view of the future. It offers a fresh look at how key global trends might develop over the next 15 years to influence world events. The report is not meant to be an exercise in prediction or crystal ball-gazing. Mindful that there are many possible "futures," it offers a range of possibilities and potential discontinuities, as a way of opening minds to developments some might otherwise miss. Some preliminary assessments are: The whole international system, as constructed following WWII, will be revolutionized. Not only will new players, Brazil, Russia, India and China, have a seat at the international high table, they will bring new stakes and rules of the game. The unprecedented transfer of wealth roughly from West to East now under way will continue for the foreseeable future. Unprecedented economic growth, coupled with 1.5 billion more people, will put pressure on resources, particularly energy, food, and water, raising the specter of scarcities emerging as demand outstrips supply. The potential for conflict will increase owing partly to political turbulence in parts of the greater Middle East. As with the earlier NIC efforts, such as *Mapping The Global Future 2020*, the project's primary goal is to provide US policymakers with a view of how world developments could evolve, identifying opportunities and potentially negative developments that might warrant policy action. The hope is that this paper stimulates a broader discussion of value to educational and policy institutions at home and abroad.

1. *Joint Operating Environment (JOE): Trends and Challenges for the Future Joint Force Through 2030* United States Joint Forces Command, December 2007.

"The Joint Operating Environment (JOE) is a historically informed, forward looking effort to discern most accurately the challenges we will face at the operational level of war, and to determine their inherent implications." The report includes such topics as: Trends Influencing the Words Society, which are, Demographics, Globalization, Economics, Energy, Food, Water, Climate Change and Natural Disasters, Pandemics, Cyber, and Space. Potential Challenges and Threats, such as China, Russia, Pacific and Indian Ocean areas, Europe, Central and South America, Africa, The Middle East and Central Asia.

1. Vallance, Chris. "US seeks terrorists in web worlds" BBC News, March 3, 2008.

This article briefly discusses the possibility of terrorist organizations using online game's/world's to coordinate their activities. It refers to a project codenamed Reynard which looks for anomalous activity in such online arenas. However, it also states that it is extremely unlikely that a terror group would use any of the existing online worlds as they are too unsecure, but to expect something like World of Jihad in the future.

1. O'Brien, Natalie. "Terrorists Practice on Cyber Game" *The Australian*, July 31st, 2007

This brief article discusses the possibility of terrorists using Second Life, an online virtual world set up in 2003 and now having over 8 million member from around the world. It states that three known Jihadi's and two elite Jihadi groups are registered on Second Life as well, and that they have turned to the online world after the United States broke up their training camps in Afghanistan.

1. Kerbaj, Richard, et al. "Dangerous and Depraved: Pedophiles Unite With Terrorists Online" *The Times Online* October 17th, 2008.

This article looks at the possible link between terrorists and pedophiles, including the possibility that terrorists are using pictures of sexually abused children to send secret encoded messages buried inside the picture. It notes that "One area that British anti-terror investigators are now keen to look at is the startling similarity in the way that jihadis and paedophiles target vulnerable young people." The article mentions it might be worth doing further research into the possible link between the two.

1. Blakely, Rhys and Jonathan Richards. "UK Headed for Cyber 'Cold War'" *Times* Online. November 29th, 2007

This article looks at a new study showing computer systems, both government and military are coming under increased sustained attack from China and other countries. It states that UK has entered a "cyber cold war" and that web-bases espionage now poses the biggest threat to national security, NATO even admitting all 26 of its member countries have been targeted by some form of cyber attack.

1. Landler, Mark and John Markoff. "Digital Fears Emerge After Data Siege in Estonia" *The New York Times*, May 29, 2007.

This article goes in depth into looking at the massive cyber attack on the country of Estonia during the end of April and beginning of May 2007, what some describe as the first, 'cyber war' in cyberspace. It detail the attack, starting from a massive Denial of Service attack using mass spam E-Mails to a giant 'botnet' attack using computers from around the globe. This is a good indication of what might happen in the future prior to an invasion of a foreign country.

1. Markoff, John. "Before the Gunfire, Cyber Attacks" *The New York Times*, August 13th, 2008

This article is similar in nature to the above one on Estonia, with the big exception that the cyber attack in this case preceded and continued throughout the Russian invasion of Georgia. It details how the attacks were carried out and that they were a precursor to the invasion and then a actual part of the attack.

1. Alexander, Keith B. "Warfighting in Cyberspace" *Joint Forces Quarterly* 46:58-61 Third Quarter, 2007

This article looks at the importance of strategies being implemented in the cyberspace arena. It puts special attention on many of the military agencies that are ramping up operations such as US Strategic Command, which establish the Join Functional Component Command for Network Warfare.

1. Anne E. Kornblut, Anne E. "Staff Finds White House in the Technological Dark Ages" *The Washington Post* January 22nd, 2009

This Washington Post article points out that the current White House is so behind on its technology that it's like "going from an Xbox to an Atari". There is no Facebook which was a staple of the Obama campaign,no instant messaging, no external access to E-Mail, etc. All things that Obama used heavily to great success in his campaign for President, and is now going to have to overhaul the White House with.

1. Janczewski, Lech J. and Colarik, A.M. "Cyber Warfare and Cyber Terrorism"

   Idea Group, Inc. 2008

Enormous efficiencies have been gained over the past twenty-five years as a result of the introduction of computers and telecommunications technologies. The use of these systems and networks translates into a major concentration and centralization of information resources, however, this consolidation creates a major vulnerability to a host of attacks and exploitations. Cyber Warfare and Cyber Terrorism reviews related problems, issues, and presentations of the newest research in this field. Cyber Warfare and Cyber Terrorism provides an overview with basic definitions of cyber terrorism and

information warfare, along with recommendations on how to handle these attacks. It presents detailed discussion on primary target facilities, deliverables, external penetration, starting points for preparations against attacks, and planning security systems. The book gives a solid introduction to cyber warfare and cyber terrorism in the 21st Century. It is a must-have for information technology specialists and information security specialists who want a first hand briefing on developments related to cyber warfare and cyber terrorism attacks.

1. Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues" CRS Report for Congress. May 20, 2007.

This report describes the emerging areas of information operations, electronic warfare, and cyberwar in the context of U.S. national security. It also suggests related policy issues of potential interest to Congress.

1. Thomas, LTC Timothy L., U.S. Army (Ret.) "Countering Internet Extremism"

The author examines the modern informational environment, and introduces the concept of contemporary extremist work as a type of living influence laboratory. He focuses on a specific Web-based counter-ideology example, then presents a methodology to address specific cyber audiences.

1. Thomas, LTC Timothy L., U.S. Army (Ret.) "China's Electronic Long Range Reconnaissance" *Military Review* Nov-Dec 2008

This article looks at China's People's Liberation Army's constant attacks on the U.S. cyber systems along with such countries as Germany, England, France, Japan, Taiwan, Australia, and others. "The article explains the Chinese military's thought's that supports their cyber-attack activities. While other articles focus on who was attacked and how many times, this article focuses more on the theory behind the attacks, especially the PLA's use of electronic stratagems for their computer network operations and the use of surrogates such as patriotic hacker groups. The article reviews Chinese incursions since 2005 and examines open-source assessments provided by some of the most important Chinese information warfare theorists."

1. Hendrson, Scott. "Beijing's Rising Hacker Stars…How Does Mother China React?" *IOsphere* Fall 2008 pp. 25-30

Mr. Henderson examines a major hacker organization in the People's Republic of China, exploring the linkages between government and private network exploitation. He reviews political, military, and economic targets, and warns against using a Western model to explain intricate online behaviors and motivations.

1. Thomas, Timothy L. "Cyberskepticism: The Mind's Firewall" *IOsphere* Spring 2008 pp. 4-8

Mr. Thomas examines various forms of computer network-related deception, including technical and social exploitation. He examines how deceptive practices can be easily concealed within existing cultural and network constructs. Finally, he advises adoption of a proper mental framework to help defeat this class of cyber threats.

1. Thomas, Timothy L. "Hezballah, Israel, and Cyber PSYOP" *IOsphere* Winter 2007 pp. 30-35

The author analyzes the evolving phenomenon of cyber psychological operations, examining their application in the recent Israeli campaign against Hezballah. He describes CYOP forms and contents, and how these capabilities enhance both insurgent and friendly influence operations.

1. DeYoung, Karen. "Obama's NSC Will Get New Power" *Washington Post* February 8, 2009 p. A1

The author reports proposed changes in the structure and authority of the National Security Council. The result will be to bring organizations such as the Departments of Energy, Commerce, and Treasury and the nation's law enforcement agencies into the security community on an issue-by-issue basis, but limit direct access to the President largely to the National Security Advisor.

Appendix A: A Question of When

The futurist who predicted 9/11 identifies 30 scenarios by which terrorists may attack us next time

By Marvin Cetron, Ph.D.

Newsmax

December 2007

The tragic events of 9/11 could have been mitigated, or possibly avoided altogether, had the government paid more attention to a little-known study called *Terror 2000: The Future Face of Terrorism*.

In that report, which I prepared for the Department of Defense in 1994, forecasters and terrorism experts warned that terrorists were planning to use commercial aircraft as guided bombs to strike against major landmarks.

Specifically, we warned that terrorists could hijack a commercial airliner and fly it into the Pentagon. Indeed, the report detailed almost every type of major terrorism event that has happened since.

Tragically, the report was filed and forgotten. Why? The State Department requested that our reference to terrorists using a jet aircraft as a weapon be deleted. They feared that it might give the terrorists an idea they hadn't already thought of.

I no longer worry about giving the bad guys ideas. They are smart and dedicated. They will think of any attack we can, and probably several others as well. That is why I am writing this article: I can't help but think that if our call for tighter security had been heeded, the Worlld Trade Center towers might still be standing today. Having the experts watching potential targets isn't enough. We need to get as many eyeballs on them as possible.

Ordinary citizens need to know where the dangers lie.

Every indication is that the terrorists' determination to hurt America is undiminished. According to the FBI and other agencies, Islamic extremists are constantly evaluating where to strike next.

This analysis of the prime targets of terrorism is based on a new Forecasting International study carried out for the Pentagon. We surveyed terrorism specialists, retired generals and admirals, futurists, and others to assess U.S. vulnerabilities. None of this information is classified.

Of the 30 threats that emerged, we give special attention to 10. To make the point that even non-nuclear threats have dire consequences, we intentionally passed on the "suitcase" nuclear weapon and dirty-bomb scenarios. Instead, we focus on the most diabolical plots for which people are least prepared.

And we lay out the scenarios in all their horrific detail.

As a citizen, you may never have an opportunity to phone in a tip that heads off a major terrorist attack. But at least by reading what follows, you will be better prepared for what could lie ahead.

Make no mistake: The men and women of our armed forces — combined with steadfast and diligent efforts of the CIA, the FBI, and many other agencies — are doing a fine job trying to protect us. Even they agree, however, that the question isn't whether America will be attacked again on its own soil. It's only a question of when.

Attack on U.S. Oil Refineries

Probability: High

Impact: High

Four terrorists driving minivans approach the gates of four oil refineries: the Royal Dutch Shell installation at Port Arthur, Texas; the Valero Energy refinery at Corpus Christi,

Texas; the Chalmette refinery east of New Orleans; and the Chevron refinery at Pascagoula, Miss. They crash through the gates and aim for the key catalytic units used to refine petroleum. The crashes set off more than 500 pounds of dynamite in the back of each van. Eleven workers die in the initial attacks and six more perish in the infernos that send plumes of dark smoke miles into the sky. Even before the flames can be extinguished, the price of oil skyrockets to more than $200 a barrel. The president declares a state of emergency and dispatches National Guard units to protect key infrastructure.

Casualties: Seventeen dead, 34 wounded (several critically burned).

Consequences: In a single day, America loses 15 percent of its crude-oil processing capability for more than a year. The Federal Reserve slashes the prime rate by a full point in a desperate attempt to avert a recession, as gas jumps to $4 a gallon. Critics bemoan the fact that, for decades, the United States neglected development of its “dirty” oil-processing infrastructure — and now it’s too late. Total economic cost: $1.2 trillion.

Attack U.S. Olympic Teams in Beijing

Probability: High

Impact: LOW

At 10 p.m. on Aug. 24, 2008, Olympians gather in the 91,000-seat National Stadium in Beijing for the closing ceremony. Americans, with more than their share of medals, are looking forward to a triumphant return home. It is not to be. As the teams enter the stadium, nine Pakistani extremists, wearing thin explosive vests made from components smuggled into China, approach the Americans and detonate suicide bombs.

Casualties: Twenty-three American athletes are killed instantly. Four more athletes die of their injuries in a Beijing hospital and two will never walk again.

Consequences: The hard-won U.S.-Pakistan alliance against terror is damaged irreparably. The Bush administration is ripped in the media for not providing adequate security to protect U.S. athletes, and Democrats appear to be headed for a clean sweep in the November elections.

Destroy Tennessee Valley Authority Dams

Probability: Low

Impact: High

The Douglas Dam stretches 1,705 feet across the Tennessee River northeast of Knoxville, Tenn. The Norris Dam spans 1,860 feet across the Clinch River northwest of

the city. On May 10, 2009, with water levels at their annual peak, a bomb far below the water line cracks the Norris Dam. An hour later, the Douglas Dam is hit.

Both structures give way, and the subsequent deluge easily sweeps away the smaller dams at Melton Hill and Fort Loudon. Some 2.1 million acre-feet of water cascade down the Tennessee Valley, sweeping away just about everything in its path. The flood plows into the Watts Bar Dam, then the Chickamauga, the Nickajack, and on down the Tennessee River. The Watts Bar and Sequoyah nuclear power plants are flooded. Debris pours out of reservoirs, flooding Chattanooga as the crest passes. No trace is ever found of the terrorists who set the bombs.

Casualties: Surprisingly, thanks to an early alert that the dams were failing, only 43 people die in this attack.

Consequences: Damage to the Chattanooga area is estimated at $5 billion. Luckily, there are no radiation leaks from the nuclear plants — but all the secondary hardware outside the containment vessels is destroyed. About 20 percent of the TVA's power-generating capacity will be out of commission for at least a year, with power-repair costs expected to run at least $2 billion.

Over the next five years, the Tennessee Valley will incur about $1 billion in flood damage the lost dams would have prevented. Cost to replace them: at least $25 billion.

Coordinate Suicide Shootings at Major Tourist Attractions

Probability: High

Impact: Low

It is Dec. 1, and families across the United States are packing in a last Saturday of vacation fun before returning home to spend Christmas with relatives. In Anaheim, Calif., two recently hired Disneyland employees stand back-to-back and begin methodically firing their AK-47s into the surrounding crowd. To avoid detection, they smuggled the weapons into work, a few pieces at a time over the past few weeks, and reassembled them. Similar attacks take place simultaneously at Walt Disney World, Universal Studios, and SeaWorld in Orlando, and at Dollywood in Pigeon Forge, Tenn.

Casualties: Before armed security personnel kill the attackers, 84 vacationers lie dead and another 103 are wounded, many critically.

Consequences: Its icons of innocence smashed, America loses hope of life returning to how it once was. Theme parks across the country lose an average of 10 percent of their business for the next year, an impact of about $1.25 billion. With many Americans afraid to resume normal lives, the economy teeters on the brink of recession.

Bring Down Four High-Tension Wires Across the West

Probability: High

Impact: High

The North American power grid has a dark secret: Of the 10,000 power substations, a loss of only 4 percent will disconnect almost two-thirds of the entire grid. But with proper planning and timing, only 2 percent need be disrupted — downing just a few power lines can have widespread consequences.

Some attacks are as easy as starting forest or grass fires under transmission lines, to ionize the air and cause the lines to fail. Others require suicide car bombs. In 12 hours, by downing just four lines, more than 60 percent of North America is without power. Power is lost from Knoxville, Tenn., to Nevada, and north to the Canadian border.

Casualties: Other than the suicide bombers, there are no direct casualties. But patients in hospitals, nursing homes, and even on respirators and other life-saving devices in private homes begin to expire. The indirect death toll starts to climb rapidly. Based on prior blackouts, 100 to 300 deaths are likely. Stop lights don't work, gas stations can't pump fuel, and civil disturbances occur as crowds waiting in lines to receive ice grow restless. The president considers requesting help from the National Guard to maintain order.

Consequences: Nearly 200 million people are affected, and infrastructure damage could take several months to repair. Even the most optimistic projections show the economic impact could easily top $100 billion.

Explode Liquefied Natural Gas Tanker and Storage Depot Near Boston

Probability: Medium

Impact: Very high

A four-seat Cessna 172 takes off from Hanscom Field in Bedford, Mass., and turns southeast. In minutes it passes over downtown Boston and arrives above the Distrigas liquefied natural gas depot on the far side of the Mystic River, in Everett.

The small craft climbs steeply, then dives at a tanker that has just begun to unload almost 40 million gallons of liquefied natural gas. On impact, a detonator sets off 250 pounds of explosives in the plane's back seat. Exploding with the power of more than 50 Hiroshima bombs, the entire storage depot is destroyed.

Boston's North End simply ceases to exist, along with parts of Chelsea, Everett, and Somerville.

Casualties: Within half a mile of the terminal, nearly everyone dies; at one mile, the toll averages 75 percent. In all, an estimated 197,525 people are lost, with thousands more injured.

Consequences: Severe damage stretches for two miles in each direction. Several billion dollars worth of property is lost, including Boston City Hall and the Faneuil Market tourist area.

The catastrophe dwarfs Hurricane Katrina by comparison. And the pain won't go away any time soon. Lacking natural gas for heat, nearly 300 elderly residents die of cold during the winter. The tourists stop coming, businesses fail, and pundits sadly remark that Boston may never again be the proud, bustling city it once was.

Introduce *E. coli* Into Fast-Food Restaurants on Wall Street and Capitol Hill

Probability: High

Impact: Low

After a costly E. coli outbreak, one major fast-food chain announces that it will start "on-the-farm" testing of lettuce. Another touts its program for preventing food-borne illnesses. Neither grasps the obvious, that their people are the weakest link — food preparation and delivery. Staff turns over rapidly at the chains, and it doesn't take long to plant "sleepers" in more than a dozen fast-food chains near Wall Street, and four within half a mile of Capitol Hill. One Wednesday morning, they start misting lettuce, tomatoes, onions, pickles, and even buns with a spray containing *E. coli*. Because the vegetables and buns are served raw, cooking will not defuse their toxins.

Casualties: With the three- to eight-day incubation period, which masks the attack and puts the initial response over a weekend, five days' worth of customers are sickened, more than 13,500 in all. They include four congressmen and two senators who, too busy to eat out, asked staffers to bring them a burger when they came back from lunch. At least 142 people die, many of them children and elderly.

Consequences: Lawsuits filed against the affected chains demand a total of $250 billion in damages. They will drag on for years. Even more costly: Fast-food hamburger orders drop by 27 percent, on average, throughout the industry for the first six months after the incident — a loss of some $57.5 billion in revenue. Once again, people ignore officials' pleas for them to get their lives back to normal.

Detonate EMP Bombs in the Internet-Critical Region of Northern Virginia

Probability: Medium

Impact: High

EMP means “electromagnetic pulse,” a blast of radio energy so strong it fries electronic equipment. (Set off an atomic bomb at an altitude of 30,000 feet, and there won’t be a computer working for miles around.) The terrorists who strike Northern Virginia on 9/11 in 2010 do not need a nuclear weapon to shut down the region’s computers. Instead, they use homemade EMP generator-bombs that any good engineering student can build with $400 and information found on the Internet. They detonate nine of the bombs within a triangle stretching from McLean west to Dulles International Airport and south to Chantilly. The EMP blasts take down communications and navigation equipment at Dulles, some of the less critical computers at CIA headquarters in Langley, and data centers that carry some 40 percent of the world’s Internet traffic. With police unable to use radios, computers, and cellphones, the terrorists escape. It is eight months before they are identified. Only one of the six-member team will be captured in the next two years. A similar bomb, detonated near Wall Street, acts as a “weapon of mass disruption,” sowing chaos and fear.

Casualties: None directly. In Northern Virginia-area hospitals, 17 patients die in part because their computerized monitors no longer operate properly. Another 14 may have died when their pacemakers delivered massive shocks to the heart and then ceased working.

Consequences: Dulles-bound aircraft are diverted for three days until replacement gear can be brought in. Some 40 percent of the world’s Internet traffic flowed through this part of Northern Virginia. Losing that capacity slows the Internet to a crawl, which further complicates emergency response.
Most of the 175,000 people employed in this IT-intensive region will be out of work for at least a year. Repairing the electronic infrastructure will cost an estimated $40 billion. Businesses across the United States lose an additional $2 billion per month owing to the loss of efficient Internet service. The Dow plummets 1,000 points and trading is suspended for three days.

Introduce Nerve Gas Into Air Ducts of Crowded Public Buildings

Probability: Low

Impact: High

A terrorist gets a low-level job servicing HVAC equipment — heating, ventilation, and air conditioning — for a contractor in Manhattan. His work takes him to important buildings: Madison Square Garden, where Andrea Bocelli is in concert; and to Carnegie Hall, where Reinbert de Leeuw is conducting students from Juilliard and the Weill Institute of Music. Also on his route: the studios and offices of ABC, CBS, and Dow Jones. Hidden in his thermos is odorless sarin nerve gas, frozen into ice cubes.

All he has to do is leave the ice inside each building’s ventilation units, which he sets to “recycle” instead of drawing in fresh air from outside. As he escapes to New Jersey, the ice melts and the deadly gas spreads through each building. Other terrorists drop vials

of pungent mercaptan, to simulate a natural gas leak, throughout Battery Park and South Street Seaport. This distracts police and emergency crews for hours. Chaos rears its ugly head in New York City.

Casualties: Of 15,000 people in Madison Square Garden, two-thirds are seriously ill and 2,851 die. At Carnegie Hall, all 600 people are sick, and 127 die. The office buildings are hit during the night shift and add 86 more deaths.

Consequences: People are terrified by the extended hyperactive coverage. Tourism and event attendance drop precipitously across the country. New York City alone loses $500 million in wages and taxes for every 1 percent decline in visitor spending. The entire hospitality industry in New York hovers on the brink of collapse.

Cruise the East Coast, Releasing Anthrax

Probability: Medium

Impact: High

Two young men enter the country from Canada at Portal, N.D. On a night with a brisk easterly wind, they drive from Boston to Washington, D.C. Opening the rooftop vent of their van, they fasten a dryer vent hose into it.

Using a small air compressor and a funnel, they send anthrax spores into the wind.

They have smuggled in only a small fraction of the weaponized anthrax stolen in Iraq after the fall of Saddam Hussein. But it will be enough. Driving through every rest area, with detours through downtown Hartford, New Haven, New York, Trenton, Philadelphia, and Wilmington, they finally arrive in Washington. Parking at the Iwo Jima memorial, they distribute the last of the anthrax and walk off.

Throughout the Northeast, the healthcare system collapses under the needs of the dying.

Casualties: According to a 2003 Pentagon report, almost 1.6 million people up to 40 miles downwind from Interstate 95 could be affected. Of those who inhale the spores, at least 95 percent will die.

Consequences: Based on the 2001 anthrax scare, this attack could restrict access to substantial areas of the Northeast for the years it would take to decontaminate more than 20,000 square miles. Cleanup and medical costs could reach $1.4 trillion.

Sidebar: The 20 other high-risk targets

According to a diverse panel of top experts, this is how terrorists are most likely to come after us.

Forecasting International, of Falls Church, Va., asked terrorism specialists, retired American generals and admirals, professional futurists, and hospitality-industry executives to assess U.S. vulnerabilities to terrorist attacks. They evaluated: 1) the likelihood of any given attack occurring; and 2) the nationwide consequences should the attack take place. The result: this list of 20 other high-risk targets.

Probability: High

Impact: High

• Attack Saudi oil production

• Conduct a suicide attack on six strip malls, then ring the malls with bombs to hit the fleeing crowds and police who respond

• Stage tanker truck “accidents” on bridges across the Mississippi, the Hudson, or other major rivers

• Bomb three oil pipelines

Probability: Medium

Impact: High

• Shoot down Air Force One

• Use an EMP to knock out financial or credit-processing systems

• Coordinate attacks on chlorine tanks at three or four sewage-treatment plants

Probability: Low

Impact: High

• Put a “suitcase” nuke at any target

• Strike at symbolic targets such as the Golden Gate Bridge, Seattle’s Space Needle, or the Statue of Liberty

Probability: High

Impact: Medium

• Pack stolen radiological medical waste around a conventional explosive, and set it off in Manhattan

• Attack six schools, synagogues, or churches simultaneously

• Attack trains full of hazardous chemicals as they pass through cities

• Take out vehicle and train tunnels leading in and out of a major city

• Poison the food at a major resort or conference center during a gathering of CEOs and/or politicians

Probability: Medium

Impact: Medium

• Bomb a chemical plant upwind of a major city

• Take out a major cruise ship entering or leaving the harbor in Miami

• Contaminate American products in foreign markets

Probability: High

Impact: Low

• Set major arson fires in six national parks near urban areas

• Detonate truck bombs at five truck stops, impacting hazardous cargoes

• Use mosquito-abatement trucks to spread pathogens — just contaminate the tanks and let the regular workers do the dirty work

This entry was posted on Wednesday, March 18th, 2009 at 6:54 pm and is filed under Articles. Both comments and pings are currently closed.