USAWC STRATEGY RESEARCH PROJECT

IDENTIFICATION -- FRIEND OR FOE?
THE STRATEGIC USES AND FUTURE IMPLICATIONS OF THE REVOLUTIONARY NEW ID TECHNOLOGIES

by

Mr. Richard K. Pruett
United States Department of State

Lieutenant Colonel Michael Longarzo
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Identification - Friend or Foe? The Strategic Uses and Future Implications of the Revolutionary New ID Technologies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Richard Pruett**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**32**	

ABSTRACT

AUTHOR: Mr. Richard K. Pruett

TITLE: Identification -- Friend or Foe? The Strategic Uses and Future Implications of the Revolutionary New ID Technologies

FORMAT: Strategy Research Project

DATE: 26 April 2006 WORD COUNT: 7,949 PAGES: 32

KEY TERMS: Counter Insurgency Operations, Information Technology, National Values

CLASSIFICATION: Unclassified

Recent developments in identification (ID) technologies are likely to have a revolutionary impact on American society and the manner by which it wages war.

The good news is that broader and more creative use of the new ID technologies could enable coalition forces to achieve dramatic victories in the Global War on Terrorism (GWOT) by targeting directly and effectively a critical requirement of most insurgencies: the insurgents' anonymity.

The bad news is that these same technologies may be inherently inimical to the future of privacy and American civil liberties. They could transform our nation and others into surveillance societies, concentrating in the hands of central governments levers of control without parallel in human history.

How to reconcile American interests and values with the imperative to bend every element of national power in their defense is the central paradox of the GWOT. Are the new ID technologies useful means to the important end of securing the United States against potentially cataclysmic attacks, or will they subvert the very interests and values at the core of all we seek to defend?

IDENTIFICATION -- FRIEND OR FOE?
THE STRATEGIC USES AND FUTURE IMPLICATIONS OF THE REVOLUTIONARY NEW ID TECHNOLOGIES

Recent developments in identification (ID) technologies are likely to have a revolutionary impact on society and the manner by which it wages war. Broader and more creative use of the new ID technologies could enable coalition forces to achieve dramatic--perhaps even decisive—victories in the Global War on Terrorism (GWOT), by targeting directly and effectively the insurgents' anonymity. The technologies could bring society a host of other benefits, as well, but critics concerned about the implications for privacy and civil liberties caution against entering into what they warn is a Faustian bargain. It is imperative that our policymakers weigh carefully the benefits and perils these attractive, new technologies pose to American society before they become pervasive.

Primarily through the support of the U.S. Department of Defense (DoD), consumer packaged goods manufacturers, and mass merchandisers, ID technologies are maturing rapidly, paying immediate dividends in the areas of supply chain management, access control, and force protection. As their associated costs continue to drop, expanded adoption of these technologies will make possible new, more value-added applications that could be enormously beneficial to society.

Critics of the technologies, however, argue that adoption of the technologies could lead to the virtual extinction of privacy. Some even fear their abuse will effectively lead to our enslavement in an Orwellian[1] "surveillance society." Although frequently dismissed by some in the security industry as alarmists and Luddites, this relatively small number of privacy advocates is attracting more and more attention in the Congress and the media.

Because the roll-out of much of this technology is already underway, the window of opportunity for public debate and timely legislation to help shape its development and uses is quickly closing. Our civilian policymakers and military leadership urgently need to look behind the industry's gee-whiz marketing literature and the privacy advocates' demonizing to gain an objective understanding of the emerging operational environment. Our elected leaders, in particular, need to educate themselves on these issues in order to establish the appropriate types and levels of risk we are willing to accept as a people.

Those risks likely will be substantial, for perhaps never before has the age-old balance between security and liberty been more precarious yet more obscure. My hope is that this paper will help, in some modest way, to sharpen understanding of these issues, especially by those involved in mitigating the risks that the use or nonuse of these new technologies could

pose, not only to the immediate safety of the American people, but to the broader ends of America's national security strategy, core interests, and fundamental values.

The New ID Technologies – Emerging Capabilities Leading to Staggering Possibilities

A few years ago, a U.S. Air Force general boldly predicted: "In the first quarter of the 21st century [we] will be able to find, fix or track and target in near real-time anything of consequence that moves or is located on the face of the Earth."[2] That prediction is rapidly coming true through the combination of new identification technologies with other information technologies, such as micro-processing and data storage, sensors, global positioning systems (GPS), and new software tools and techniques, such as data mining and link analysis. The strategic and social ramifications of this emerging capability merit considerably more attention than they have received.

The most significant of the new ID technologies are biometrics and radio frequency identification (RFID).

Biometrics measures an individual's unique distinguishing physical characteristics, reduces them to digital data, and then compares them in "one-to-one" matching with those measurements in templates previously recorded in a database. The most mature biometric technologies involve fingerprint, iris, hand geometry, face, and voice recognition.[3] Although named by *MIT Technology Review* as one of the "top 10 emerging technologies that will change the world,"[4] biometrics is not entirely new; the ancient Chinese used fingerprints to authenticate property deeds, and the early Egyptians used them to authenticate pottery.[5]

Especially since the late 1990s, dropping data storage costs have enabled biometrics' reemergence in several, primarily governmental and military applications, including force protection, access control, workforce maintenance, and detention center monitoring. The use of biometrics also is increasingly common in the marketplace, where, for example, millions of Americans can now cash checks, buy gas, or purchase groceries with a touch of their finger at thousands of retailers across the United States.[6]

As a leader in the development of biometrics, the United States is in a good position to leverage its application to the GWOT. The Quadrennial Defense Review Report of 2001 listed biometrics as among the most promising emerging technologies that DoD plans vigorously to develop and exploit "for tracking adversaries and providing secure authentication of individuals seeking network or facility access."[7] In fact, biometric techniques provide the technical underpinning for large-scale civil status and identity "smart "card projects now being pursued

around the world[8] and may be incorporated in the de facto national ID card for the United States mandated in the Real ID Act of 2005.[9]

A new, biometrics-based national identity "Multipurpose Access Card" proposed for the citizens of Iraq would link to a central database tied to various existing Iraqi governmental databases, and would be used for such purposes as vetting, checkpoints, access control, forgery detection, detainee security, decentralized verification and entitlements.[10] A similar project aiming at using a biometrics-based identification card for purposes of force protection should be available to coalition forces by December 2006.[11]

The United States already is compiling biometric measurements of local workers and terrorism suspects in Afghanistan, in the streets of Iraq, and at our incarceration facility at Guantanamo Bay, Cuba, using the Biometric Automated Toolset developed by the Battle Command Battle Laboratory at Ft. Huachuca, Arizona. DoD's Automated Biometric Identification System allows this biometric information to be compared with that contained in the world's largest biometrics database, located at the U.S. Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System facility located in Clarksburg, West Virginia.[12]

The potential of this technology increases exponentially when combined with RFID technology. Like biometrics, RFID is not entirely new; it was used during World War II in "Identification Friend or Foe" (IFF) systems to differentiate between friendly and hostile aircraft.[13]

RFID transponders, or "tags," consist of a computer chip and a micro-antenna. These can be embedded directly in an item or in a tiny plastic attachment and configured to lie passive until passing within activation range of a compatible reader/scanner. At that point, the tag silently beams its Electronic Product Code (EPC), and any other information it was programmed to relay, back to the reader for processing. Direct line of sight is not required. A battery-operated, active version also is available, including one using a printed battery less than a millimeter thick.[14] The maximum operating range between tags and readers is limited and depends on many factors, including the radio frequency being used, the amount of power emitted by the reader, and the degree of radio interference in the vicinity. Passive tags are readable within only a few meters. Active versions provide dramatically increased range, typically up to dozens of meters.[15]

Unlike the now-common barcode, which identifies stock-keeping units only, RFID tags allow identification of specific items. The 96-bit EPC can allow discrete IDs for 2^{96} different

objects, equivalent to 80,000 trillion trillion objects, more than enough for every man-made object in existence.[16]

Many of the largest consumer product manufacturers in the world have already entered into RFID contracts and are working toward interoperability, driving the cost of producing RFID tags down toward the industry goal of a few cents apiece.[17] In June 2003, Wal-Mart threw its weight behind RFID by requiring its top suppliers to begin attaching RFID tags to their Wal-Mart shipments by 2005.[18] In July 2004, DoD's Total Asset Visibility initiative gave RFID another huge boost by mandating its use by January 2005 in products going to distribution depots.[19]

Low cost RFID, in combination with low cost data storage, could allow RFIDs to be placed on a vast number of objects, opening the way to "pervasive computing" (also known as "ubiquitous computing"), in which computers would become integrated into the environment, animating otherwise inert objects.[20] This "embodied virtuality" will allow for greater human-computer and computer-computer interaction. It will also allow for an "Internet of objects," in which, as ludicrous as it may sound, "a can of beans will come with its own individual webpage…"[21]

The ability to track individual items using RFID will likely improve every link in the supply chain--perhaps even dramatically--from manufacturing to retail distribution and even disposal. RFID could eliminate most inventory theft or loss, provide better shelf-life monitoring, assist in product recalls, promote "just-in-time" inventory management, secure baggage handling, identify discarded parts for salvaging, and help to achieve a variety of other efficiencies. The introduction of networked RFID readers in the home (in the form of "smart " appliances, furniture, medicine cabinets, ceiling tiles, etc.), would allow for the monitoring of food, medicines, belongings …and even occupants, for purposes such as care-giving.[22] Some privacy advocates fear this capability could be abused for purposes of marketing or coercive government control.

RFID already is the enabling technology behind "smart tags" at toll booths, "speed passes" at gas stations, and tracking tags on millions of pets …but this is just a hint of its potential. As Accenture puts it: "Almost any physical item can be embedded with electronic tags and sensors to establish a unique and verifiable identity, store a wealth of information, and sense changes in the environment."[23]

For example, RFID tags can combine with a whole class of tiny, networked, wireless sensors, called "smart dust" and "motes," to monitor heat, light, movement and other environmental factors. Motes are already being used in transportation and viticulture. Using microelectromechanical systems for locomotion, and distributed intelligence to produce "swarm

behavior" similar to the collective behavior of insect colonies, a meshed “colony” of low-observable motes could share magnetometer information, peer-to-peer, in order to provide early warning of an advancing tank column or a possible ambush. Sown in a future battlespace by the thousands, at a cost of only about $1 apiece, they would be too numerous to destroy and, at perhaps the size of a grain of sand, too small to notice. Deriving their power from sunlight, vibrations, or perhaps just a coating of radioactive isotopes, they could have greater longevity than humans. Their military missions could include such things as sniffing out deadly toxins, hunting missiles, or monitoring treaty compliance.[24]

With the emerging ability to tag nearly everything with its own unique identifier and to track it using RFID, the possibilities for vastly expanded surveillance are staggering. So, too, though, would be the concomitant amounts of storage required to retain the data generated. Then there is the matter of developing software sophisticated enough to sort through what would amount to a series of massive, global databases, in order to find those proverbial “needles” in the “haystack.”[25]

Thanks to the plunging cost of data storage, a number of huge databases already exist or are under development. In fact, in 2004 the world’s largest database was owned by Wal-Mart and already contained more than twice as much data as the entire Internet combined.[26] Some observers estimate that the world’s storage of data roughly doubles in quantity every year. [27]

Sophisticated data analysis tools now offer the ability to sort quickly through mountains of data and to tie disparate data to individuals using the new forensics attribution capability made possible by biometrics and RFID. Commonly referred to as “data mining,” these are actually part of a larger process known as “knowledge discovery in databases” or KDD, which examines relationships among data using a variety of parameters, including association, sequence or path analysis, classification, clustering, and forecasting.[28]

A now-disbanded military intelligence unit code-named “Able Danger” reportedly used KDD techniques to identify terror suspects (including four of the 9/11 hijackers) operating in the United States some 18 months before September 11, 2001. Attempts by Able Danger team members to share their information with the FBI in 2000 apparently were blocked by Pentagon lawyers due to concerns over domestic intelligence gathering.[29]

The Total Information Awareness (later renamed “Terrorism Information Awareness,” or TIA) project, headed by former National Security Advisor Admiral John Poindexter under the Information Awareness Office (IAO) at the Defense Advanced Research Projects Agency (DARPA), was designed to fight terrorism through data mining and link analysis, and by exploiting such technologies as “biometric signatures of humans” and “human network

analysis."[30] In practical terms, this meant that it would attempt to identify terrorists by linking databases, then scanning for suspicious activity the financial, medical, travel, and government records of millions of Americans. Alarmed by the implications, Congress cut off appropriations to IAO in September 2003. IAO's less controversial technologies were transferred to other DARPA offices.[31]

The expansion of databases and effective data mining techniques, combined with biometrics and RFID, are making technologically possible for the first time the positive identification and tracking of virtually everyone and everything on Earth. We need to examine further the implications of this new capability. Following is a brief ends, ways, and means analysis of the risk posed by the new technologies in the context of today's strategic environment.

The Strategic Environment: A Time of Profound Transition with Danger and Opportunity

The collapse of the Soviet Union and the rise of pan-Islamic extremism in the new context of the "Information Age" and globalization have ushered in a period of profound transition characterized by volatility, uncertainty, complexity, and ambiguity. Although a certain degree of vertigo is common to any fin de siecle or millennial period, few serious observers doubt that the international security environment is experiencing a shift of seismic proportions. Indeed, some believe the international system may be undergoing its greatest transition since the Treaty of Westphalia in 1648 and the very creation of the modern nation-state.[32] Some have even argued that the Westphalian system is obsolete, that nation-states are incapable of governing effectively the global market forces now emerging.[33]

Despite the present turmoil, many remain optimistic that the global diffusion of knowledge at the heart of globalization will eventually lead to a "richer, healthier, safer, more educated, and more stable world…,"[34] a view consistent with the Socratic identification of knowledge with virtue that long has influenced Western thought.

Thomas Friedman has been a leading proponent of the view that globalization will lead to greater individual freedom and political decentralization. Yet, even in his popular book about globalization, *The Lexus and the Olive Tree*, published in 2000, Friedman gave voice to a new and nagging anxiety:

> If the defining anxiety of the Cold War was fear of annihilation from an enemy you knew all too well in a world struggle that was fixed and stable, the defining anxiety in globalization is fear of rapid change from an enemy you can't see, touch or feel—a sense that your job, community or workplace can be changed at any moment by anonymous economic and technological forces that are anything but stable.[35]

The fear of "anonymous forces" became less nebulous on the tragic morning of September 11, 2001. The outrages perpetrated by al-Qaeda that day ended America's sense of complacency regarding trends in the new security environment. They also brought a degree of much-needed clarity, as many confronted for the first time the uncomfortable fact that the forces of globalization had helped to catalyze and facilitate a new challenge of global terrorism -- rendering frighteningly plausible the specter of nihilists, masked in anonymity and intent on killing Americans, in possession of weapons of mass destruction.

In self-defense, the United States adopted a policy the Bush Administration has euphemistically termed "preemptive war," but which, in fact, amounts to preventive war. It is a strategy with which many Americans and our allies are uncomfortable, but as President Bush has stated: "History will judge harshly those who saw this coming danger but failed to act."[36] In the new security environment, the Government's failure to use any single element of national power could have catastrophic consequences.

The transformation of terrorism is an aspect of globalization's transformation of crime. The faster movement of people, products, and ideas—what some call the "end of geography"[37]—has heightened the risks of fraud, theft, smuggling, drug trafficking, human trafficking, counterfeiting, and money laundering. It has led to an explosion in cases of identity theft,[38] computer intrusion (using worms, viruses or phishing),[39] and thefts of customer financial and other account data.

This environment of high tech-empowered criminality has provided fertile ground for the growth of new identification and tracking technologies. Moreover, the increased "friction" in global supply chains caused by tightened security has only increased the need for the stronger supply chain management the new technologies offer. The U.S. Department of Energy used RFID early on for tracking fissionable materials.[40] DoD's inability to track supplies in Operation Desert Storm, which resulted in the stacking of thousands of containers in "iron mountains" in Gulf ports and the waste of billions of dollars, led to DoD's Total Asset Visibility effort to use RFID "to be able to pinpoint the location and content of every plane, ship, tank, and cargo container in transit around the world."[41] The need to secure the integrity of container shipping led to the Smart and Secure Tradelanes initiative dictating the sealing of containers at their port of origin with RFID tags.[42]

Another impetus globalization has given to the development and deployment of the new ID technologies is the increased risk of pandemic. The recent Severe Acute Respiratory Syndrome (SARS) and Avian Flu Virus scares have confirmed the danger of pandemic, first demonstrated by the rapid, global spread of the Acquired Immune Deficiency Syndrome in the

1980s. Positive identification is critical to the main tactics for containing pandemics, which consist of case-finding, quarantine, contact tracing, and close control of border chokepoints.[43] Taiwan and Singapore already are using RFID chips to control SARS by tracking everyone who comes into contact with SARS patients.[44]

Because secure borders are essential to guarding against pandemic and international criminality, the world community's movement toward incorporating the new ID technology in travel documents is well underway. In the Enhanced Border Security and Visa Act of 2002, the U.S. Congress imposed a requirement for the 27 countries participating in the Visa Waiver Program (VWP)[45] to begin using tamper-resistant, machine-readable passports incorporating biometric and RFID technology. The new passport would comply with interoperable biometric standards adopted by the International Civil Aviation Organization. The Congressional deadline for compliance by VWP countries has been extended to October 26, 2006. By the summer of 2006, the U.S. Department of State hopes to begin issuing "e-passports" incorporating the same technology, after it first perfects safeguards designed to prevent the passports from being read surreptitiously by anyone with the right scanner.[46]

Our leveraging of America's visa waiver partners, in order to promote the use of the new ID technologies for purposes of national security, may prove to be a paradigm for the coming age. Nation-states may not be as effective as before at staunching the flow of capital or ideas, but they still define territory and citizenship. The ability of states to exercise some aspects of sovereignty may be eroding, but networks of states acting collectively still can institute far-reaching security and other measures that can actually strengthen their prerogatives.

The Ends: Advancing Core American Interests and Values in a Safer and Better World

This period of sweeping change is a time of great opportunity for promoting what Americans regard as universal values. President Bush has espoused this view, stating:

> Today, the international community has the best chance since the rise of the nation-state in the seventeenth century to build a world where great powers compete in peace instead of continually prepare for war…. The United States will use this moment of opportunity to extend the benefits of freedom across the globe. We will actively work to bring the hope of democracy, development, free markets, and free trade to every corner of the world. [47]

The goals of U.S. national security strategy are "to help make the world not just safer but better," and include "political and economic freedom" and "respect for human dignity." These are worthy goals, based--as the overview of the strategy asserts--"on a distinctly American internationalism that reflects the union of our values and our national interests."[48] The strategy

argues from American first principles, as enshrined in our Declaration of Independence and protected in our Constitution:

> In pursuit of our goals, our first imperative is to clarify what we stand for: the United States must defend liberty and justice because these principles are right and true for all people everywhere. No nation owns these aspirations, and no nation is exempt from them. Fathers and mothers in all societies want their children to be educated and to live free from poverty and violence. No people on earth yearn to be oppressed, aspire to servitude, or eagerly await the midnight knock of the secret police.
>
> America must stand for the nonnegotiable demands of human dignity: the rule of law; limits on the absolute power of the state; free speech; freedom of worship; equal justice; respect for women; religious and ethnic tolerance; and respect for private property. [49]

Similarly, the *National Strategy for Combating Terrorism,* published in February 2003, concludes by stating:

> The defeat of terror is a worthy and necessary goal in its own right. But ridding the world of terrorism is essential to a broader purpose. We strive to build an international order where more countries and peoples are integrated into a world consistent with the interests and values we share with our partners—values such as human dignity, rule of law, respect for individual liberties, open and free economies, and religious tolerance. We understand that a world in which these values are embraced as standards, not exceptions, will be the best antidote to the spread of terrorism. This is a world we must build today. [50]

In short, the broader purpose of the U.S. national strategy for combating terrorism is to create conditions necessary for a world consistent with the interests and values we share as Americans. Moreover, wider acceptance of those values will help to prevent future acts of terrorism.

How to reconcile those interests and values with the imperative to bend every element of national power in their defense is the central paradox of the GWOT. It is also the point of departure between the proponents and opponents of the new ID technologies.

The conflict over the uses of identification is an identity conflict in the larger sense, for the supporters of the technologies see them, inter alia, as useful means to the important end of securing the United States against potentially cataclysmic attacks, while the opponents of the technologies fear they will subvert the very interests and values at the core of all we seek to defend.

<u>The Ways: Know the Enemy and Know Yourself</u>

In some ways, our strategy for combating terror will say as much about us as it does about the enemy. The Chinese strategist Sun Tzu's oft-quoted dictum "know the enemy and

know yourself"[51] is as valid today as it was 2500 years ago. We need to "shape" the enemy while understanding our own character, with all its strengths and weaknesses.

Through study, observation, and interrogation, we have learned much about al-Qaeda's tactics, infiltration routes, weapons of choice, ideology, etc. Nonetheless, most of us would not recognize a suicide bomber if he sat at the opposite table from us in a café--until it was too late, that is (as I discovered for myself during a particularly disagreeable lunch in Baghdad in 2004).[52] Although al-Qaeda's top leadership is relatively visible, we cannot readily distinguish its rank-and-file from others we might encounter on patrol. Even al-Qaeda's leader in Iraq, Abu Musab al-Zarqawi, reportedly was detained in 2004 but released for lack of recognition.[53] We need to know the enemy. At present, we often do not even recognize him.

Even in the theoretical realm, there is disagreement regarding what constitutes the enemy's strategic "center of gravity" or COG.[54] The largest body of scholarly U.S. military opinion argues that ideology is al-Qaeda's strategic COG,[55] but the *National Defense Strategy* lists the terrorists' ideological support as a vulnerability, which, according to some U.S. military doctrinal precepts, by definition should rule it out as a COG.[56]

To regard ideology as the enemy's COG may be to perpetuate the common doctrinal mistake of confusing the concept of COG with that of "critical vulnerability." Numerous studies suggest that al-Qaeda's support stems less from its violent ideology than from other factors, such as the Islamic world's youthful demographics, high unemployment, alienation from local elites, low quality of education, growing urbanization, and rapid—if belated—modernization.[57] In fact, studies suggest that a majority of Moslems actually have a high regard for the American people and for American products and values.[58]

We should recognize that the GWOT is, in the long run, a war of ideas. We also should recognize that every war of ideas is a long run, indeed. Whether we regard ideology as the enemy's COG or a critical vulnerability, we need to de-legitimize terrorism in order to dry up the state and private support of those who use it as a tactic. Yet, it is very difficult to destroy an idea, and the question remains whether, in waging such a war, we can win quickly and decisively enough to protect ourselves from the terrorist use of WMD. We are unlikely to stamp out al-Qaeda—much less terrorism as a tactic—any time soon. Although embracing absolutist and particularistic values often directly antithetical to those generally promoted through globalization, al-Qaeda and other extremist groups have proven adept at using the anonymity afforded by the Internet in order to establish on-line "emirates"[59] that facilitate recruitment, linkage with like-minded organizations, and dissemination of their views. As long as the United States remains the world's most puissant nation, Christian in heritage, allied with Israel, and a

champion of tolerance, pluralism, and gender equality, it is probable that some Islamist extremists will link together with a view to waging *jihad* against it, the arguments of orthodox religious leaders notwithstanding. Even if the war of ideas goes well and the number of terrorists dwindles, there would be little comfort in knowing that a terrorist organization in possession of WMD has a membership numbered in the hundreds rather than the thousands.

Moreover, we have not been faring so well in the war of ideas. Our government's explicit doctrine of preemptive war, its policies regarding incarceration of "illegal combatants," the tactics used at Abu Ghraib prison, the "extraordinary rendition" of prisoners to other countries, the Patriot Act's expanded police powers (including national security letters, "sneak and peek" search warrants, and roving wiretaps), the revelation of domestic spying by the National Security Agency, and the subpoena of Internet browsers continue to raise questions among some about the compatibility of American values and "nonnegotiable demands of human dignity" with the manner by which the U.S. Government is prosecuting the GWOT.

Setting aside the merits of the individual issues, it is an irony that, while our government follows a strategy in Iraq designed to isolate the enemy politically, some of its tactics have tended to weaken abroad the support of our coalition partners and to alienate at home the support of the American people. They also have tended to diminish the attractiveness in the Islamic world of the American way of life as a model for emulation and as a yardstick against which to measure the conduct of our enemy.

Although isolating the enemy politically is a fundamentally valid approach, toward which we have made some progress, it would be far more effective if we could isolate him physically. Until now, we have been unable to do so because of the enemy's anonymity.

Anonymity is an oft-overlooked but critical requirement for most insurgencies. The characteristic of anonymity is arguably the true center of gravity for most insurgencies, as it is typically the leading source of the insurgents' power and their ability to maneuver.

Anonymity allows the insurgent to attack unexpectedly, to hide after striking, and to escape punishment, like a serial killer who masks his murderous persona with banality. Anonymity confers on him the illusion of ubiquity. Because he can appear anywhere and yet is nowhere to be found, he can strike with near-impunity, which greatly enhances his essential capability to intimidate. It is small wonder, then, that today -- as with the Viet Cong a generation ago -- our enemies prefer to cloak themselves in anonymity, even at the risk of forfeiting their legal combatant status.[60] In fact, many insurgents may choose terrorist tactics in preference to conventional operations precisely for fear of disclosing their true identities.

All of our range, speed, maneuverability, stealth, precision, firepower and willpower avail us naught if we do not know the identity of our enemy and his location. Were we able to pierce the enemy's veil of anonymity, to know his identity and to trace his location, we could swiftly defeat him. The new identification technologies might offer us those means.

The Means – Securing the Battlespace by Leveraging Information Dominance

A suicide bomber intent on achieving his version of martyrdom may not be capable of being deterred; with sufficient actionable intelligence, however, he can be stopped. Conversely, "knowing that the event can be traced to its planner and executor … can create strong inhibitions in those that are not personally suicidal."[61] The means to achieve these early warning and forensic attribution capabilities could soon be multiplied greatly by using the new ID technologies in a variety of ways.

Perhaps the most effective way is through the combined use of a biometrics-based national identity card system, pervasive computing (using RFID and KDD), and more traditional investigative "skip-tracing" techniques. This would constitute probably the purest example of a "System of Systems Analysis" approach ever attempted in warfare, using "networks to fight networks."[62] Employing principles of operational net assessment and effects-based operations, it would accomplish joint preparation of the battlespace by creating for the combatant commander and his joint staff a common operational picture in which the entire range of the enemy's political, military, economic, social, infrastructure, and information systems are mapped, using the new ID technologies for positive identification of enemy assets, or nodes, and KDD for links analysis and targeting.

Imagine these technologies' application to a now all-too-familiar scenario where a car bomb explodes in a marketplace. RFID readers at various sites around the market had earlier recorded the car's arrival in the marketplace by reading EPCs from passing RFID tags embedded in the vehicle's tires and windshield. Other EPCs were recorded at nearly the same instant. A comparison of the readers shows that each had recorded the same sets of EPCs as the car passed by. Investigators are disappointed to learn that none correspond to a biometric ID card or valid license plate, but some of the EPCs correspond to apparel and others to currency, which also can be tracked. By querying RFID readers at chokepoints throughout the area, the vehicle's EPCs are traced back to a suburban garage that surveillance soon reveals is a bomb-making factory. Purchase records and previous RFID readings of the other EPCs implicate an individual who has been an occasional visitor to the garage. He had left his biometric ID at home on the day of the bombing, but his shoes, shirt, and wallet all contain RFID

chips that silently revealed his movements to readers located at the various chokepoints. Continued surveillance of the factory and the suspect yield a long list of related EPCs for additional tracing.

The decision whether and when to raid the factory and/or arrest the suspect is part of the commander's operational art. He will need to design non-linear Rapid Decisive Operations (RDO) focused against the enemy's nodes and links and to choose the decisive point at which to attack using synchronized, discriminate, and proportionate force or other measures.[63] The operations would seek to peel back the enemy's nodes and links, exposing sub-nodes and sub-links for further exploitation after the measurement of effects and the appropriate re-alignment of resources.

The commander would do well to wait. This would allow him to map out the enemy's entire shape, using his scalable constellation of RFID readers and other sensors to detect and record more and more links among an ever-expanding network of nodes. The delay also would allow his staff time to use KDD tools to drill down deeper into archived data, in order to identify additional target sets, build legal cases for prosecution, and develop planning sequels for RDOs designed to roll up the enemy network with minimal risk to noncombatants.

This strategy would allow us to sort the insurgent out from the general population or, at the very least, cause him to take evasive measures tending to isolate him from society and commerce. It is an electronic version of the blockhouse and wire fence strategy used by the English in the Second Boer War and the *quadrillage* system used by the French to win the Battle of Algiers in 1957. It would enable us to isolate the enemy and force him to move like a "roving bandit," susceptible to capture at every identification chokepoint, whether it be a local dragnet, a turnstile, a grocery checkout counter, or an RFID reader hidden along a road.[64]

Because this will be the first such application of the new ID technologies, great surprise is achievable. Opposing forces literally will not know what hit them, except that they somehow were tipped off to the authorities. Until they understand and take countermeasures against the technologies, it will be possible to use the waves of arrests to stay within the enemy's decision cycle, or "OODA loop,"[65] sowing distrust and disunity in their ranks through "epistemological," "neo-cortical warfare"[66] tactics such as bond-relationship targeting.

Such an operation would be a watershed for netcentric warfare – the transition of information dominance from force multiplier to new capability.[67] It would serve as a prime example of netwar, truly akin to playing the oriental game of Go with full visibility of all of the stones, while one's own are screened from the adversary's view.[68]

The foregoing scenario is not far-fetched. There are other possibilities, as well. For example, strewn among the rocks beside a goat trail in Waziristan, movement-sensing smart dust could trigger surveillance overflights or alert rapid response teams. The dropping cost of RFID technology and data storage should make such scenarios possible in a few short years.

The Defense Science Board Task Force on Identification Technologies would like to speed the process. Last year, it advised Defense Secretary Donald Rumsfeld to fast-track these technologies, because winning the GWOT would require "a 'Manhattan Project'-like tagging, tracking, and locating" program for potential security threats.[69]

Risk – The Potentially Prohibitive Costs of Unintended Consequences

The success of the Manhattan Project radically changed the operational environment. Before launching a program of comparable scope in the area of identification technologies, it would prudent to weigh the possible second- and third-order consequences.

As the *National Defense Strategy* notes, some objectives, though desirable, may not be attainable, while others, though attainable, may not be worth the costs.[70] Are the powerful, new ID technologies desirable but not attainable? Can these or any technologies really provide a "silver bullet" for the GWOT, or would their adoption by DoD only validate the criticism that it is unable to shift from a netcentric to a culture-centric warfighting paradigm?[71] Conversely, are the technologies attainable but not worth the costs? The costs need to be weighed very carefully, especially since the same technology could, and almost certainly would, be used in the United States, for and against American citizens.

In *United States v. Olmstead*[72] in 1928, Supreme Court Justice Louis Brandeis' dissent referred to "the right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men." It is difficult to see how a system of surveillance as pervasive and invasive as that created through the use of these technologies can be anything but inimical to this right.

Yet some feel that encryption and other technologies will moderate many of the risks to privacy. There are even those who suggest that more distributed inverse surveillance of authority figures, or "sousveillance" (watching from below), can serve as a counter to panoptic surveillance and a check on abuses of authority, as in the case of a citizen's 1991 videotaping of Rodney King's beating by Los Angeles police. Already the wide use of camera phones may enable citizens to conduct more effective neighborhood watch systems. Some observers point to this as an early version of the "equiveillance," or harmonious balance between surveillance and sousveillance, that pervasive computing and worn (or implanted) computers will bring to

society. Privacy is sacrificed but greater transparency is achieved, leading to better accountability and a purer form of democracy. [73]

A futurist recently lecturing at the Army War College[74] may have been thinking of equiveillance when he enthused that globalization is carrying us toward "a free society with civil liberties safeguarded by everybody watching everybody else--a panopticon." Perhaps he had forgotten that the panopticon devised by philosopher Jeremy Bentham was far from a free society. It was, in fact, a prison designed to mold behavior through the use of pervasive surveillance.[75]

Justice Brandeis also warned: "Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent…. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[76] Especially by using the Social Security number as a de facto identification number--contrary to numerous assurances[77]--the federal government for many years has incrementally expanded its power to compel sharing of personal information, always citing favorable political transaction costs to the public (e.g., "this measure will reduce welfare fraud, crack down on illegal immigration, penalize deadbeat dads, etc."). The new ID technologies seem to promise even greater benefits. With the ability to track virtually everyone and everything, governments may be poised to strengthen their ability to exercise sovereignty by defeating terrorism, reducing crime, preventing money laundering, verifying entitlements, and creating secure--perhaps almost seamless--border crossings.

The market, too, will operate more efficiently, achieve greater integration, and possibly even transition to a cashless society. This degree of integration and interoperability will imply supranational organization and regulation, raising the question whether a world integrated enough to accept one universally interoperable card might be a short step from a single world government—a long-cherished dream to some but anathema to others.

Although many people believe that only "bad guys" need fear national IDs or other ID technology, privacy advocates and libertarians on both ends of the political spectrum are alarmed. Few see world government as imminent, but all distrust government, however benevolent its stated intentions. Of course, it is because America's Founding Fathers shared that fundamental distrust that they chose to predicate our Constitutional system of "checks and balances" on the idea that government is a necessary evil that must be limited. At a minimum, uncertainty regarding governments' uses of personal information fosters anxiety and conformity[78] -- not without cause, since even the United States used census records to segregate Japanese-Americans during World War II. In the hands of totalitarian and genocidal

governments, the new ID technologies could be quite lethal -- "*die Gedanken sind frei*" replaced by "*Information macht frei*." In fact, during the violent 20th century, state power directed by governments against their own citizens was responsible for more democide than war.[79] What is to prevent the new ID technologies from being bent to the same malevolent purposes, again raising the question once asked by Juvenal: "*Sed quis custodiet ipsos custodes*" [Who will guard us from the guardians]?

Standing in stark relief to the optimistic views of the future of globalization now prevalent, this dark vision of a digital gulag posits that, far from witnessing the eclipse of the Westphalian nation-state system by the rising, pluralistic influence of non-state actors, we instead may be on the threshold of an information counterrevolution that will lead to unprecedented concentrations of state power and their possible transformation into one or more supranational entities. For those with political leanings to the Right, the bogey tends to be a single world government menacing to American ideals; for those on the political Left …a fascist consortium of governments and the military-industrial complex.

Many fundamentalist Christians share a conviction that RFID technology will migrate from smart cards to subcutaneous implants (voluntary at first but later mandatory), and that these implanted chips will correspond in Biblical prophecy to "the mark of the Beast" in *Revelation* 13:16-17.[80] Some believe that the sinister number '666,' signifying the prophesied "number of the Beast" of *Revelation* 13:18,[81] already is encoded in UPC codes.[82] Those who refuse the chip will be regarded with deep suspicion and will experience persecution--the "Great Tribulation"--having been effectively locked outside the world economy.

It would be easier to dismiss these apocalyptic fears as paranoid were it not for the fact that Applied Digital Solutions has been implanting FDA-approved RFID "VeriChips" in humans for years, marketing them for use in medical emergencies and to combat kidnapping. It has implanted thousands and now has no less than former Health and Human Services Secretary Tommy Thompson serving as its pitchman.[83]

VeriChips are not very different from the over 15 million microchips already implanted in animals.[84] This leaves some to wonder: with the Pentagon turning to the use of microchips in military "dog tags,"[85] and dogs now being tagged with chip implants, what will be next -- implants as the generation-after-next military dog tag?

Profoundly disturbing or profoundly disturbed, such concerns hint at the depth of antipathy the new ID technologies will encounter from at least some segments of the population. In fact, a privacy activist has predicted "a resistance – along the lines of what happened in France in World War II" within five years, "if logic and common sense doesn't prevail."[86]

For now, what seems to be prevailing, instead, is an atmosphere of accusation and recrimination between privacy activists and industry stakeholders, with most other people either indifferent to the technology or oblivious to it altogether. If awareness should only come with personal exposure, by that time the technology presumably will be firmly established in the market.

Recommendations – The Need for Risk Mitigation and Balance

Although a broad spectrum of interoperability, durability, and other technical and regulatory difficulties[87] continue to hamper the pace of the new ID technologies' development, they are a present, not a future, challenge. It is too late for Luddite tactics; the technology is already here. The task now is to mitigate the risks posed by these technologies even as we weigh those risks against the technologies' usefulness in the GWOT.

Able Danger illustrated the general dilemma and the high stakes involved. Had Able Danger's reported use of KDD techniques not been blocked due to concerns over domestic intelligence, might the 9/11 hijackings have been averted? Similarly, if now we do not exploit the potential of the new ID technologies, we may be leaving the door open to even greater catastrophe. On the other hand, how much domestic intelligence should Americans accept? We could undermine our own strategic center of gravity -- the national will – if we adopt an approach to prosecuting the war that will lead more Americans to feel alienated from their own government.

Recognizing the new ID technologies as a potent weapon, but also as a new category of vulnerability, we must develop new safeguards to protect consumer and personal privacy before it is too late. The first step is to recognize and confront the issues. The Department of State's decision to modify its new passport technology in order to lessen vulnerability was such a step, but much more needs to be done. A report released by the Government Accountability Office (GAO) in September 2005, for example, noted incredulously that, although 13 government agencies are using or plan to use RFID, only one identified any legal or privacy issues with the technology. GAO then went on to summarize "several security and privacy considerations that may affect federal agencies' decisions to implement the technology."[88] The Privacy and Civil Liberties Oversight Board, created by Congress in December 2004 at the urging of the 9/11 Commission, should devise an interagency process to introduce privacy standards as well as to protect against overly intrusive security practices by federal agencies.

It may well be that we shall need to make trade-offs at the expense of privacy for the sake of security, but that line should be drawn by our elected representatives after full and informed

debate. Especially while it is prosecuting a war, the Executive branch of government cannot be relied upon alone to serve as a sufficient check on its own powers. Independent judicial review would ease some concerns, but the Constitution, Supreme Court precedents, current privacy law, and tort law do not offer much guidance regarding the challenges to privacy protection posed by the new technologies. It is Congress that is best able to provide the necessary oversight and direction.

Congress ended Admiral Poindexter's TIA program. It also canceled the Computer Assisted Passenger Prescreening (CAPPS) program, which would have used data mining to assign risk to airline passengers based on their data profiles. When Congress extended the Patriot Act last July, lawmakers inserted a provision requiring that the Justice Department report annually to Congress on the use of data mining. It needs to do more, such as to broaden the applicability of the 1974 Privacy Act to the new ID and data-mining technologies,[89] determine to what degree and to what ends official and commercial databases can be mixed, decide who can access these databases and under what conditions, etc.

Congress, state legislatures, and some local jurisdictions have made various attempts to legislate privacy standards for RFID, typically to mandate disclosure and to give consumers the choice to opt out.[90] Some members of the RFID industry have endorsed these efforts, while lobbying by other members has succeeded in stymieing them, usually by arguing against "premature" restrictions on an infant industry before any real harms have been demonstrated.[91]

Those arguments notwithstanding, this is precisely the time that standards should be legislated, with the understanding that they likely will need adjusting over time. As Paula J. Bruening of the Center for Democracy and Technology put it in congressional testimony:

> [I]t is more effective and efficient to begin at the outset of the development process to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed, rather than building in privacy after a scandal or controversy erupts publicly. [92]

Today, civilization faces implacable enemies of proven ruthlessness and resourcefulness, against which the new identification technologies may constitute a particularly potent weapon. Yet, will the technology fulfill our brightest hopes or realize our darkest fears, instead? Will knowledge so pervasive lead man toward Socratic virtue or, alternately, to Sophoclean hubris? Perhaps Vaclav Havel was right to say that globalization is morally neutral; it can be good or bad, depending on the kind of content we give to it.[93] In view of the stakes, we need to choose that content wisely. America's elected leaders, in particular, need to assess the feasibility and suitability of these technologies, and, thus informed, debate the acceptability of their various

uses in American society. American society needs to recognize and mitigate their inherent risks now, lest we soon discover that, in the process of targeting our enemies' identities, we have sacrificed our own.

Endnotes

[1] George Orwell, *1984* (New York: Harcourt, Brace, Jovanovitch, Inc., 1949). In his 1983 preface to its republication, Walter Cronkite writes: "If not prophecy, what was *1984*? It was, as many have noticed, a warning: a warning about the future of human freedom in a world where political organization and technology can manufacture power in dimensions that would have stunned the imaginations of earlier ages."

[2] U.S. Air Force Chief of Staff General Ronald Fogelman, quoted in Kenneth R. Israel, "1998 Airborne Reconnaissance," available from: http://www.global-defense.com/1998/SurveillanceCounter/1998.htm; Internet; accessed 3 January 2006. USAF Major General Israel was Director of DoD's Defense Airborne Reconnaissance Office.

[3] James Jay Carafano, "The Future of Anti-Terrorism Technologies," *Heritage Lectures*, No. 885 (Washington, DC: The Heritage Foundation, June 6, 2005), 3-4.

[4] John D. Woodward, Jr., "High-Tech Human Identification Can Fight Terrorism," *Pittsburgh Post-Gazette*, September 24, 2001, repeated in RAND Corporation Commentary, available from: http://www.rand.org/commentary/092401PPG.html; Internet; accessed 18 September 2005.

[5] Bernard Didier, "Biometrics," in Organisation for Economic Cooperation and Development (OECD), *The Security Economy* (ISBN 92-64-10772-X: OECD, 2004), 36.

[6] See "Pay by Touch to Acquire Biopay, Strengthening Both Companies' Value to Retailers and Consumers," 06 December 2005 Press Release at: http://www.paybytouch.com/news/pr_12-06-05.html; Internet; accessed on 7 January 2006.

[7] United States Department of Defense, *Quadrennial Defense Review Report* (September 30, 2001), 38-39.

[8] Most of the world's countries now have a national ID system. (Source: Jennifer Pero, "Tools Exist--from Biometrics to Smart Cards--that can Verify a Citizen's Identity, but at What Cost?," *Government Security*, 22 July 2002; available from: http://govtsecuritysolutions.com/ar/security_6/, Internet; accessed 21 September 2005.)

[9] The act establishes national standards for state-issued drivers licenses and non-drivers identification cards. Cards must incorporate "a common machine-readable technology, with defined minimum data elements." Although unnamed, many observers believe this technology will involve biometrics. See http://en.wikipedia.org/wiki/REAL_ID_Act; Internet; accessed 08 March 2006.

[10] Carol A. Haave, "Iraq Multipurpose Access Card," presentation at U.S. Embassy, Baghdad, dated 27 July 2004.

[11] United States Department of Defense, "Contracts," No. 502-05, (Washington, D.C.: U.S. Department of Defense Public Affairs, 23 May 2005), available from: http://www.defenselink.mil/cgi-bin/dlprint.cgi?http://www.defenselink.mil/contracts/2005/ct20050523.html; Internet; accessed 15 February 2006.

[12] Jim Krane, "U.S. Military Building Database of Terror Suspects' Fingerprints, Faces, Voices," Associated Press, October 29, 2002, available from: http//www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2002/10/29/national1456EST0653.DTL; Internet; accessed 21 February 2006. Also see Dawn S. Onley, "Biometrics on the Front Line," Government Computer News, Vol. 23, No. 23, 16 August 2004, available from: http//www.gcn.com/23_23/top-stories/26930-1.html; Internet; accessed 22 September 2005. Also see Gerry J. Gilmore, "DoD Prepares Biometric ID System for U.S. Bases in Iraq," Armed Forces Press Service, Washington, 17 May 2005, available from: http//www.af.mil/newws/story.asp?storyID=123010540; Internet; accessed 22 September 2005. Also see http://www.sodaro.com/Plone/bat_news/newsitem_view?month:int=7&year:int=2005; Internet; accessed 26 April 2006. Also see John D. Woodward, Jr., "How do you know friend from foe?," *Homeland Science & Technology* (December 2004).

[13] United States Department of Commerce, *Radio Frequency Identification: Opportunities and Challenges in Implementation* (Washington, D.C.: U.S. Department of Commerce, April 2005), 5. RFID is again being considered for IFF purposes. The U.S. Defense Department hopes to use radio frequency tags to give every allied soldier and weapons platform a unique IFF identifier to answer queries from laser range finders. This would complement or supplant the Army's Blue Force Tracking system now used for battlespace visualization. See Noah Shachtman, "Friend or Foe? A Digital Dog Tag Answers," *The New York Times*, 15 April 2004; available from: http://www.nytimes.com/2004/04/15/technology/circuits/15next.html?ei=5007&en=7ee72093df747330&ex=1397361600&adxnnl=6&partner=USERLAND&adxnnlx=1117858285-1/Oi1Kefl+5eipqzmH7e2A; Internet; accessed 15 January 2006.

[14] "LLC and TBT Announce Partnership to Develop Printed Batteries," press release, Precisia website, available from: www.precisia.net/news/precisia_news_20040506_01.html; Internet; accessed 7 February 2005, also cited in Katherine Albrecht and Liz McIntyre, *Spychips* (Nashville, Tennessee: Nelson Current, 2005), 18.

[15] Didier, 57-58.

[16] David Brock, "The Compact Electronic Product Code: A 64-Bit Representation of the Electronic Product Code," (Cambridge, Massachusetts: MIT Auto-ID Center, 1 November 2001), Massachusetts Institute of Technology White Paper, available from: http://www.quintessenz.at/rfid-docs/www.autoidcenter.org/pdfs/MIT-AUTOID-WH-008.pdf; Internet; accessed 21 February 2006.

[17] Kevin Maney, "New chips could make everyday items 'talk'," *USA Today*, 12 April 2002, 8A.

[18] A similar policy in the 1980s was essential to the successful introduction of bar codes. Today, some 87% of all supermarket items are bar coded. See: Laurie Sullivan, "RFID Implementation Challenges Persist, All This Time Later," *InformationWeek* , 10 October 2005; available from: http://internetweek.cmp.com/shared/article/printableArticleSrc.jhtml?articleId=172300306; Internet; accessed 21 December 2005. See also: Alorie Gilbert, "Wal-

Mart tagging fuels RFID market," *News.com* , 22 December 2004; available from: http://news.com.com/Wal-Mart+tagging+fuels+RFID+market/2100-1012_3-5501432.html; Internet; accessed 16 January 2006.

[19] Chantal Polsonetti, "US Department of Defense Issues Updated RFID Policy," *ARC Wire*, 11 August 2004; available from: http://www.arcweb.com/community/indnews/display.asp?id= 5729; Internet; accessed 16 January 2006.

[20] See Mark Weiser, "The Computer for the Twenty-First Century," *Scientific American,* Vol. 265, No. 3 (September 1991), 94-104; available from: http://www.ubiq.com/hypertext/weiser/ SciAmDraft3.html; Internet; accessed 16 January 2006. The late author is considered the father of ubiquitous computing, or "ubicomp." His website is still available from: http://www.ubiq.com/ weiser/; Internet; accessed 24 February 2006.

[21] Joseph Jofish Kaye, "Counter Intelligence/Kitchen Sync White Paper," Massachusetts Institute of Technology website, available from: http://www.media.mit.edu/ci/papers/whitepaper/ ci13.htm; Internet; accessed13 January 2006. Also cited in Albrecht, 27.

[22] Example: "By tagging key objects in a senior's home …and embedding small RFID readers in gloves that can be worn by that individual, that person's daily habits can be monitored remotely by a caregiver." Federal Trade Commission, *Radio Frequency Identification: Applications and Implications for Consumers* (March 2005), 61. It should be noted that for such a system to work, RFID readers would need to provide coverage for the house and to be connected to the Internet. Also, RFID tags would need to remain activated. See Nicholas Chavez, "The Original Spychips Rebuttal," *RFID Limited* (7 November 2005), 12; available from: www.packagedrfid.com/spychips_rebuttal.pdf; Internet; accessed 8 January 2006.

[23] "Silent Commerce Offers New Insight for High Performance," Accenture website, available from: http://www.accenture.com/Global/Research_and_Insights/By_Industry/ Health_and_Life_Sciences/Providers_and_Government_Health/PointsPerformance.htm; available from http://www.accenture.com/; Internet; accessed 8 March 2006.

[24] Rolf Clauberg, "RFID and Sensor Networks – From Sensor/Actuator to Business Application," (Rüschlikon, Switzerland: IBM Research, Zurich Research Laboratory, n.d.) Also see "In Dust We Trust," *The Economist*, 10 June 2004; available from: http://www.cis.gsu. edu/~dtruex/courses/IB8680/ArticlesandExamples/EconomicsMonitorJune1204/dust-chips.html; Internet; accessed 21 February 2006. See B.J. Feder, "Psst. This is Your Sensor. Your Grapes Are Thirsty," *The New York Times*, 26 July 2004. See Brendan I. Koerner, "What is Smart Dust, Anyway?," *Wired* Issue 11.06, June 2003; available from: http://www.wired.com/ wired/archive/11.06/start.html?pg=10; Internet; accessed 07 January 2005. See David Pescovitz, "Robugs: Smart Dust Has Legs," *Lab Notes* Vol.3, Issue 7 (Berkeley, CA: University of California at Berkeley, September 2003), available from: http://www.coe.berkeley.edu/ labnotes/0903/pister.html; Internet; accessed 08 January 2006. Kris Pister of the University of California at Berkeley is one of the developers of Smart Dust. Read his ruminations on sensor technology in the year 2010 on his Web log, available from: http://robotics.eecs.berkeley.edu/ ~pister/SmartDust/in2010; Internet; accessed 15 February 2006.

[25] As Lt. Gen. Philip Kensinger, head of U.S. Army Special Operations Forces, puts it: "What my forces have to be able to do is …continue to train and work with host-nation forces

and U.S forces and other agencies to try to establish a global intel database so that that little piece of information that you may get out of some little area, say, in Rwanda, provides the key to a cell someplace else around the world." Quoted in Linda Robinson, "Plan of Attack," *U.S. News and World Report* (August 1, 2005), 31.

[26] Constance Hays, "What Wal-Mart Knows About Customers' Habits," *New York Times*, 14 November 2004, Section 3, 1; available from: http://www.nytimes.com/2004/11/14/business/yourmoney/14wal.html?ex=1258088400&en=0605d1fc88b8ab98&ei=5090&partner=rssuserland; Internet; accessed 21 February 2006.

[27] Jeffrey W. Seifert, *Data Mining: An Overview* (Washington, D.C.: The Library of Congress Congressional Research Service, 16 December 2004), CRS-2.

[28] Ibid., CRS-1.

[29] Jacob Goodwin, "Inside Able Danger – The Secret Birth, Extraordinary Life and Untimely Death of a U.S. Military Intelligence Program," *Government Security News*, available from: http://www.gsnmagazine.com/sep_05/shaffer_interview.html; Internet; accessed 15 February 2006.

[30] *The Information Awareness Office Home Page*, formerly available from http://www.darpa.mil/iao; Internet; accessed 17 December 2002.

[31] http://www.govexec.com/dailyfed/0903/092503td1.htm; Internet; accessed 26 October 2005.

[32]For example: "In the rapidly changing international scene characterized by American military supremacy and non-state actor attack, it may be that we are entering into a rare fundamental shift in the understanding of the international system such as we have not seen in four centuries." Martin L. Cook, "Ethical Issues in War: An Overview," *U.S. Army War College Guide to National Security Policy and Strategy*, J. Boone Bartholomees, Jr., ed., (Carlisle, PA: U.S. Army War College, July 2004), 29.

[33] For example: Kenichi Ohmae, *Borderless World: Power and Strategy in the Interlinked Economy* (London: Sage Publications, 1990), 13.

[34] Among a range of views discussed in Ellen Frost, "Globalization and National Security: A Strategic Agenda," in Richard L. Kugler and Ellen L. Frost, eds., *The Global Century: Globalization and National Security* Volume I (Washington, D.C.: National Defense University Press, 2001), 35.

[35] Thomas L. Friedman, *The Lexus and the Olive Tree*. (New York: Random House, Inc., 2000), 12.

[36] George W. Bush, Foreward to *The National Security Strategy of the United States of America* (Washington, D.C.: Executive Office of the President, 2002).

[37] Zygmuni Bauman, *Globalization: The Human Consequences*, 9 (1998), quoted in Rhoda E. Howard-Hassman, "The Second Great Transformation," *Human Rights Quarterly*, Johns Hopkins University Press, 2005), 7.

[38] In March 2000, the Federal Trade Commission (FTC) received and responded to approximately 400 complaints of identity theft. Less than a year later, the FTC was logging an average of 1,700 such complaints every week. Source: Bank Secrecy Act Advisory Group, *The SAR Activity Review -- Trends, Tips & Issues*, Issue 2, (Washington, D.C.: U.S. Department of the Treasury Financial Crimes Enforcement Network, June 2001), 14.

[39] Bank Secrecy Act Advisory Group, *The SAR Activity Review -- Trends, Tips & Issues*, Issue 3, (Washington, D.C.: U.S. Department of the Treasury Financial Crimes Enforcement Network, October 2001), 15-17.

[40] United States Government Accountability Office, "Informaton [sic] Security – Radio Frequency Identification Technology in the Federal Government," May 2005, 4; available from: http://www.gao.gov/new.items/d05551.pdf; Internet; accessed 8 March 2006.

[41] U.S. Congress, House of Representatives, Congressional testimony of Daniel O. Hill, Assistant Administrator for Technology, U.S. Small Business Administration, before the Subcommittee on Technology of the House Committee on Science, 17 June 1999; available from: http://www.house.gov/science/hill_9-4.html; Internet; accessed on 3 January 2006.

[42] "Smart and Secure Tradelanes," available from: http://www.sitglobal.org/download/documents_container_security/SST_Phase2_Intro_WP.pdf#search='U.S.%20Customs%20Smart%20and%20Secure%20Tradelanes%20initiative'; Internet; accessed 21 February 2006.

[43] National HIV/AIDS Sentinel Surveillance System, "Monitoring Virtual Borders," *HIV/AIDS Surveillance, 2002 Report* (Manila, Philippines: National HIV/AIDS Sentinel Surveillance System, 2002), 2.

[44] Aubrey Hudson, "Orwellian Eyes," *The Washington Times*, 27 November 2003; available from: http://www.washingtontimes.com/functions/print.php?StoryID=20031126-113641-3955r; Internet; accessed 15 November 2005.

[45] The program enables citizens of 27 countries to visit the United States for tourism or business for up to 90 days without obtaining a visa. The 27 VWP countries are: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

[46] Sarah Lai Stirland, "State Department Official Defends Passport Efforts," *Government Executive*, 29 April 2005; available from: http://www.govexec.com/dailyfed/0405/ 042905tdpm1.htm; Internet; accessed 22 November 2005. Also see the testimony of Deputy Assistant Secretary for Consular Affairs Frank Moss at the House Hearing of the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity on "Ensuring the Security of America's Borders through the Use of Biometric Passports and Other Identity Documents," 22 June 2005; available from: http://hsc.house.gov/release.cfm?id=374; Internet; accessed 11 January 2006.

[47] Bush, Foreword.

[48] Ibid., 1.

[49] Ibid., 3.

[50] *National Strategy for Combating Terrorism* (February 2003), 30.

[51] "Know the enemy and know yourself; in a hundred battles you will never be in peril" (*Zhi bi zhi ji zhe bai zhan bu dai*.) Sun Tzu, *The Art of War* (*Bing fa*). Translated by Samuel B. Griffith, London: Oxford University Press, 1963, 84.

[52] On October 14, 2004, a homicide bomber detonated a bomb consisting of an estimated 10 pounds of high explosive encased in nails in the middle of the "Green Zone Café," just a few steps away from where I was sitting. The bombing, coordinated with another attack at a nearby market, utterly destroyed the café but resulted in only one fatality—the bomber—although many were injured, some grievously. Four American security contractors were killed in the market bombing.

[53] Robert Reid, "Al-Zarqawi was caught, released, CNN report says," Associated Press, 16 December 2005; available from: http://www.thestate.com/mld/charlotte/news/ 13419454.htm?source=rss&channel=charlotteobserver; Internet; accessed 3 January 2006.

[54] "One must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point on which all our energies should be directed." Carl von Clausewitz, *On War,* Michael Howard and Peter Paret, eds. and trans., (Princeton, NJ: Princeton University Press, 1976), 595-596.

[55] Regarding the enemy's COG as his ideology, see, for example, Antulio J. Echevarria II, *Globalization and the Nature of War*, (Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, March 2003), vii; and the following Strategy Research Projects at the U.S. Army War College: James A. Bliss, *Al-Qaeda's Center of Gravity* (Carlisle Barracks: U.S. Army War College, 3 May 2004); Stephen W. Davis, *Center of Gravity and the War on Terrorism* (7 April 2003); Joe E. Ethridge, Jr., *Center of Gravity Determination in the Global War on Terrorism* (3 May 2004); John Halberkern, *The Global War on Terrorism: Ideology as its Strategic Center of Gravity* (03 May 2004); Tim Keppler, *Center of Gravity Determination and Implications for the War Against Radical Islamic Terrorism* (18 March 2005); James Reilly, *A Strategic Level Center of Gravity Analysis on the Global War on Terrorism* (9 April 2002); and Joseph P. Schweitzer, *Al-Qaeda Center of Gravity and Decisive Points* (7 April 2003). An interesting minority view is available in John W. Jandora, "Center of Gravity and Asymmetric Conflict – Factoring in Culture," *Joint Forces Quarterly* 39, 78-83. On page 80, Jandora states that "addressing the moral [i.e., ideological] dimension would be a generational project and is, therefore, a nonstarter. On the other hand, addressing the physical dimension is more feasible and suggests two approaches: removing tribal leadership…or co-opting tribal authorities and, through them, their tribes." For an influential discourse on COG and its related concepts, see: Joe Strange, *Centers of Gravity and Critical Vulnerabilities* (Quantico, VA: Defense Automated Printing Service Center, 1996).

[56] United States Department of Defense, *The National Defense Strategy of the United States of America*, (March 2005), 8.

[57] For example: Alan Richards, "Socio-Economic Roots of Radicalism? Towards Explaining the Appeal of Islamic Radicals" (Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, July 2003).

[58] For example: Zogby International, "Impressions of America 2004", a six-nation survey commissioned by the Arab American Institute, available from: www.aaiusa.org/PDF/ Impressions_of_America04.pdf; Internet; accessed 15 February 2006.

[59] Jarret Brachman, "Internet as Emirate: Al-Qaeda's Pragmatic Use of the Virtual Jihad," *ROA National Security Report* (Washington, D.C.: Reserve Officers Association, December 2005), 95-98.

[60] "Geneva Convention Relative to the Treatment of Prisoners of War," adopted on 12 August 1949 by the Diplomatic Conference for the Establishment of International Conventions for the Protection of Victims of War, held in Geneva from 21 April to 12 August, 1949. Entry into force 21 October 1950. See Part I, Article 4, A. 2.

[61] Jay Davis, *The Grand Challenges of Counter-Terrorism* , Center for Global Security Research, Lawrence Livermore National Laboratory, 2001; available from: http://cgsr.llnl.gov/ future2001/davis.html; Internet; accessed 22 January 2006.

[62] John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND Corporation, 1997), 290.

[63] For a recent example of a successful RDO led by Iraqi security forces, see: James K. Greer, "Operation Knockout: COIN in Iraq," *Military Review*, November-December 2004, 16-19.

[64] Cf. David Galula, *Counterinsurgency Warfare – Theory and Practice* (New York: Frederick A. Praeger, 1964), 134.

[65] The "OODA loop" was a term coined by the late USAF Col. Paul Boyd. 'OODA' is short for "observe-orient-decide-act."

[66] Richard Szafranski, "Neo-Cortical Warfare? The Acme of Skill," *Military Review*, November 1994, 41-55.

[67] For a discussion of bond-relationship targeting and the transition of information operations to a new capability, see Robert J. Bunker, *Information Operations and the Conduct of Land Warfare* (Arlington, VA: The Association of the United States Army, 1998).

[68] Arquilla, 163.

[69] Paul McHale, Assistant Secretary of Defense for Homeland Defense, "Homeland Security Defense: An Update," 4th Global Homeland Security Conference and Expo: Protecting the Nation's Critical Infrastructure and Key Assets, E.J. Krause and Associates and Deloitte Consulting Conference, Bethesda, Maryland, 23 November 2004, quoted in John D. Woodward, Jr., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism," *Military Review*, September-October 2005, 32.

[70] United States Department of Defense, *National Defense Strategy*, 11.

[71] See Tony Corn, "World War IV as Fourth-Generation Warfare," *Policy Review*, January 2006; available from: http://www.policyreview.org/000/corn.html; Internet; accessed on 17 January 2006.

[72] U.S. Supreme Court, *Olmstead v. U.S*., 277 U.S. 438 (1928); available from: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=277&invol=438; Internet; accessed 12 January 2006.

[73] See Ian Kerr and Steve Mann, "Exporing [sic] Equiveillance," 1 January 2006; available from: http://wearcam.org/anonequiveillance.htm; Internet; accessed on 23 January 2006. See also: David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, Massachusetts: Perseus Books, 1998).

[74] The U.S. Army War College's nonattribution policy does not permit me to disclose the lecturer's identity.

[75] Jeremy Bentham, The Panopticon Writings, ed. Miran Bozovic (London: Verso, 1995), 29-95, available from: http://cartome.org/panopticon2.htm ; Internet; accessed 21 November 2005.

[76] U.S. Supreme Court, *Olmstead v. U.S.,* 277 U.S. 438 (1928); available from: http://caselaw. lp.findlaw.com/scripts/getcase.pl?court=US&vol=277&invol=438; Internet; accessed 12 January 2006.

[77] See Charlotte Twight, "Watching You: Systematic Federal Surveillance of Ordinary Citizens," *The Independent Review* Volume IV, Number 2 (Oakland, CA: The Independent Institute, Fall 1999), 165-200.

[78] See, for example, Paul Schwartz, "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," *Hastings Law Journal* 43, Part 2, 1992, 1374, cited in Ibid., 166.

[79] R. J. Rummel, "20th Century Democide," available from: www.hawaii.edu/powerkills/20TH.HTM; Internet; accessed 15 November 2005. In fact, one of the worst offenders, the People's Republic of China, now has one of the world's largest RFID programs. (See, for example, Chris Strohm, "Chinese government enacts unprecedented ID tag program," *National Journal's Technology Daily*, available from: http//www.nationaljournal.com/about/technology/daily; Internet; accessed 25 April 2006.)

[80] Rev. 13:16: "And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads:" (13:17) **"**And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name." (King James Bible)

[81] Rev. 13:18: **"**Here is wisdom. Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is six hundred threescore and six." (King James Bible)

[82] The left- and right-hand guard bars (the start and stop characters) and the center bar of the UPC appear identical to the encodation for the digit '6,' but there are subtle, technical

differences. See: "Bar Code 1," available from: http://www.adams1.com/pub/russadam/new.html; Internet; accessed on 13 January 2006. Also see Robert Harris, "No Hidden Sixes in the UPC Code," available from: http://www.virtualsalt.com/barcode.htm; Internet; accessed on 13 January 2006.

[83] As of this writing, Thompson apparently has not yet fulfilled his earlier promise to receive the chip implant himself. See: Brian Bergstein, "Thompson Still Open to Having Chip Implant," (Boston: Associated Press, 14 December 2005), available from: http://abcnews.go.com/Technology/wireStory?id=1406784&CMP=OTC-RSSFeeds0312; Internet; accessed 15 January 2006.

[84] Source: "EZID Animal Verification Systems," available from: http://www.ezidavid.com/products.htm; Internet; accessed on 15 January 2006.

[85] Jonathan Karl, "Pentagon introducing hi-tech dog tags," *CNN Interactive*, 27 December 1997; available from: http://www.cnn.com/TECH/9712/27/high.tech.dog.tags/index.html; Internet; accessed 15 January 2006.

[86] John Leyden, "Privacy 'Dark Ages' force activist rethink," Channel Register, 1 April 2005, available from: http://www.channelregister.co.uk/2005/04/01/privacy_resistance/; Internet; accessed 15 November 2005. The quotation is attributed to Simon Davies, a director of London-based Privacy International, which describes itself as "a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations," available from: http://www.privacyinternational.org/; Internet; accessed 15 January 2006.

[87] United States Government Accountability Office, "Defense Logistics – Better Strategic Planning Can Help Ensure DOD's Successful Implementation of Passive Radio Frequency Identification," September 2005, 24-25.

[88] United States Government Accountability Office, "Informaton [sic] Security," available from: http://www.gao.gov/new.items/d05551.pdf; Internet; accessed 7 March 2006.

[89] For an excellent briefing on how the Privacy Act can and should be amended, see: John M. Eden, "When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID," *2005 Duke Law & Technology Review* 0020, 31 August 2005; available from: http://www.law.duke.edu/journals/dltr/articles/2005dltr0020.html; Internet; accessed 22 January 2006.

[90] For the most salient example of such legislation, see: HR 4673 IH, the "Opt Out of ID Chips Act," sponsored by Rep. Jerry Kleczka (D-WI), 108th Congress, introduced 23 June 2004; available from: http://www.techlawjournal.com/cong108/ rfid/hr4673ih.asp; Internet; accessed 22 January 2006.

[91] Some elements of the RFID industry have endorsed notification and opt-in solutions as good business. For example, see: "FAQs – Q & A Section about RFID Uses & RFID Technology," *RFID Journal*; available from: http://www.rfidjournal.com/faq/28/129; Internet; accessed 22 January 2006. The Progressive Policy Institute has endorsed a "wait and see" approach but warns the industry that it must work with the federal government to establish privacy guidelines or expect legislation that could be unwelcome. See Jonathan Collins,

"Institute Warns of Rash RFID Laws," *RFID Journal*, 11 October 2004; available from: http://www.rfidjournal.com/article/articleprint/1183/-1/1; Internet; accessed 22 January 2006.

[92] *RFID Technology: What the Future Holds for Commerce, Security, and the Consumer:* Hearing Before the Subcommittee on Commerce, Trade, and Consumer Prot. of the House Comm. on Energy and Commerce, 108th Cong. 28 (2004) (statement of Paula J. Bruening, Staff Counsel, Center for Democracy and Technology), as cited in Eden at http://www.law.duke.edu/journals/dltr/articles/2005dltr0020.html; Internet; accessed 22 January 2006.

[93] Vaclav Havel, *The New York Times*, August 23, 2000, A8.