This article aims to look at information, and information technology (IT) in general, to show how certain aspects are so critical to all the homeland security [1] mission areas that, on their own, they may determine whether the outcome is a failure or a success. From preparing for to preventing a threat and from managing, responding, and recovering from an attack, the timely delivery of information has become the centerpiece to achieving success. The existing interrelations among all critical infrastructures (that currently support our way of life) are such that only with a carefully planned and executed systems-approach, both for technology and policy as well, we will be able to address homeland security effectively. Some current evolving new policies for homeland security and proposed legislation are briefly reviewed here as well because of their criticality. As we create and apply new tools, techniques, and devices to help solve our problems at hand, a set of new procedures will need to be instilled and followed, and new policies will supply the required direction and financial support needed to be enacted. The events of September 11, 2001, have acted as a catalyst creating a de facto set of new “security” requirements for data and information processing departments. No matter how big or small an enterprise may be, and regardless if it is public or private, the data it owns may have the potential to prevent an attack or even help find out who the perpetrators may be. Although we, individually, may think that “our business” is not related to homeland security, still, “our data” may provide key information to others for discovery. Of course at what price? Most Americans are concerned about terrorist threats but are as concerned regarding their privacy and the protection of their rights.

Critical “Info”-structure
Computers and communications networks not only are a critical infrastructure, but each of the areas identified as part of the (National) critical infrastructure has an information technology (IT) component. Given IT’s critical role in many other elements of the national infrastructure and in responding to a crisis, the targeting of IT as part of a multijuged attack scenario could have catastrophic consequences … Thus, complete integration is not only quite difficult, it is politically impossible and culturally undesirable. [2]

IT is essential for us to function. As shown in Figure 1, virtually every aspect of our system not only depends on IT, but there are very close interrelations among all segments. From food distribution to controlling the electric power grid, the operation and management of a nuclear plant, the gates of a dam to controlling the air traffic control system, the rail systems of trains, the opening and closing of bridges, the functioning of financial institutions, to telesurgery procedures, all depend on IT.

From the intelligence gathering to the required analysis to discovering threat perpetrators to the planning for prevention, and warning and protection of our assets there are a growing number of IT tools [3] that can provide the means to do these tasks more effectively and efficiently. Modeling and simulation, knowledge management, data mining/data warehousing, intelligent agents, decision support/ expert systems, geographical information systems/geographical positional systems, and link-analysis are just some of the tools that computer science and engineering have to offer to the homeland security community.

Converging Technologies and Critical Infrastructure Interdependencies
According to Nolan’s [4] “stages theory” we are currently in what he calls the “Network Era” (in terms of organizational learning) of the “Information Economy” in the “Period of Transformed Enterprise,” where supporting the development of intelligent products and services are the basis of the emerging demand for networks. Although some individuals predicted well over a decade ago the convergence of computers and communications networks, very few included in this vision the inclusion of television/cable and satellite TV, phones, and all sorts of mobile computing devices, i.e., laptops, PDAs, etc., with the rest of the computer systems. What implicitly may be occurring is that with this convergence there may be a slowly but steady-evolving shift on the (definition of) “critical infrastructure.” In other words, not only our interdependencies keep growing and shifting at the same time, but the requirements for interoperability keeps expanding as well [5].

In January 1991 a crew working with fiber cables in the streets of New York City accidently cut one of the cables.
Immediately 60% of the long distance calls in and out of New York City were blocked [6]. At the same time two other events occurred:
1) the air-control functions in Boston, New York, and Washington, D.C., were disabled
2) operations at the New York Mercantile Exchange and several commodity exchanges were disrupted.

The National Strategy for Homeland Security and Related Presidential Directives

Government at the federal, state and local level must actively collaborate and partner with the private sector, which controls 85 percent of America’s infrastructure. The Nation’s infrastructure protection effort must harness the capabilities of the private sector to achieve a prudent level of security without hindering productivity, trade or economic growth. [7]

The National Strategy for Homeland Security [8] released in July 2002 is a “national” strategy, not a departmental or a federal one. It outlines the roles and responsibilities for local, state, and federal government and for nongovernment stakeholders. It has 84 strategic goals, to be accomplished in six “critical mission areas” and four “foundation areas.” The critical mission areas are:
1) Intelligence and Warning
2) Border and Transportation Security
3) Domestic Counterterrorism
4) Protecting Critical Infrastructure and Key Assets
5) Defending Against Catastrophic Threats
6) Emergency Preparedness and Response

The foundations are: law, science, and technology; information sharing; and systems; and international cooperation.


Presidential Decision Directive (PDD) 63 [14], titled Protecting America’s Critical Infrastructures, was publicly released on 22 May 1998 and it set a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003 and significantly increased security to government systems by the year 2000 by immediately establishing a national center to warn of and respond to attacks and ensuring the capability to protect critical infrastructures from intentional acts by 2003. It also addresses the cyber and physical infrastructure vulnerabilities of the federal government by requiring each department and agency to work to reduce its exposure to new threats; and...
it requires the federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained. It seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships and protects privacy rights.

Analysis: Review of Policies and Rational

Homeland security directive 7 supersedes Presidential Decision Directive/NSC-63 since both focus on the protection of our critical infrastructures. However our critical infrastructures are just a subset of the homeland security mission areas. If we compare the goals and objectives of all the homeland security critical mission areas, (i.e., intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure and key assets, defending against catastrophic threats, and emergency preparedness and response) with the content of HSPD: 4, 5, 6, 7, and 8, the correlations depicted in Table 1 can be established. Some of these areas, i.e., protecting critical infrastructures, may have a very specific Presidential Directive (HSPD 7 for this example) addressing this mission. Other HSPD (s) may also affect this mission. Continuing with the example, HSPD 6 (Integration and Use of Screening Information) and NSPD 4 (National Strategy to Combat Weapons of Mass Destruction) both could have an impact from an intelligence and warning (mission) and/or defending against catastrophic threats (mission) if, for example, a critical infrastructure was attacked using a weapon of mass destruction. In addition, HSPD 7 specifically puts an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, which is specifically addressed by HSPD-4.

All mission areas rely on information sharing and information systems. These two elements are a fundamental basis for homeland security and the successful implementation of all mission areas objectives. There are important interrelations between all the critical mission areas and IT. For example “information and communication networks” are a critical infrastructure and need to be protected. If we fail to do it, then all other critical infrastructures (i.e., transportation systems, electric power grids, oil and gas delivery and storage, banking and finance, water, emergency services, government services, public health and food supplies) are in jeopardy and so are the other five critical mission areas.

Some questions worth reflecting on. When we speak of “homeland security” what are we referring to? Is it the land within the physical boundaries of the United States? Since 85% of the critical infrastructures belong to the private sector, should it follow that homeland security involves American businesses, i.e., U.S. multinational corporations and their interests, here and abroad? We have in this country brilliant individuals who are leaders in their respective fields. Their inventions and/or products produce millions of dollars in revenue in a wide spectrum of areas that may go from medical discovery (i.e., drugs to cure diseases), to the entertainment field (i.e., movies), to the computer software development field. Are they part of a “business critical infrastructure”? What about American citizens traveling abroad?

Summaries of Bills: S1230 [15] and S871 [16]

On 11 June 2003, Bill S1230, to provide for additional responsibilities for the Chief Information Officer (CIO) of the Department of Homeland Security (DHS) relating to geospatial information, was introduced in the U.S. Senate. Besides establishing and carrying out a program to provide for the efficient use of geospatial information, i.e., providing such geospatial information as may be necessary to implement the critical infrastructure protection programs and providing leadership in meeting the requirements of, and populating the databases used by, those responsible for planning, prevention, mitigation, assessment and response to emergencies, critical infrastructure and other functions of the DHS, it seeks to assure the interoperability of, and prevent unnecessary duplication of, geospatial information among all users. Under the responsibilities for DHS’ CIO is not only the managing of the geospatial information needs and activities of the DHS but also establishing such standards as are necessary to assure the interoperability of geospatial information pertaining to homeland security among all users of such information within the DHS; other federal agencies; state and local government; and the private sector.

On 10 April 2003, Bill S871, to provide for global pathogen surveillance and response, was introduced in the U.S. Senate. [The term “syndrome surveillance” means the recording of symptoms (patient complaints) and signs (derived from physical examination) combined with simple geographic locators to

<table>
<thead>
<tr>
<th>Critical Mission Area</th>
<th>Affected by HSPD</th>
<th>PDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence and Warning</td>
<td>(6) Integration and Use of Screening Information</td>
<td></td>
</tr>
<tr>
<td>Border and Transportation Security</td>
<td>(6) Integration and Use of Screening Information</td>
<td></td>
</tr>
<tr>
<td>Domestic Counterterrorism</td>
<td>(5), (8), (6) Management of Domestic Incidents, National Preparability, Integration and Use of Screening Information</td>
<td></td>
</tr>
<tr>
<td>Protecting Critical Infrastructure and Key Assets</td>
<td>(7), (6), (4) Critical Infrastructure Identification, Prioritization and Protection, Integration and Use of Screening Information, Nat. St. to Combat Weapons of Mass Destruction</td>
<td>63</td>
</tr>
<tr>
<td>Defending Against Catastrophic Threats</td>
<td>(4), (6) National Strategy to Combat Weapons of Mass Destruction, Integration and Use of Screening Information</td>
<td></td>
</tr>
<tr>
<td>Emergency Preparedness and Response</td>
<td>(8), (4), (6) National Preparedness, N.S. to Combat W. Mass Destruction, Integration and Use of Screening Information</td>
<td></td>
</tr>
</tbody>
</table>
track the emergence of a disease in a population. The Congress findings included that:

An effective international capability to monitor and quickly diagnose infectious disease outbreaks will offer dividends not only in the event of biological weapons development, testing, production, and attack, but also in the more likely cases of naturally occurring infectious disease outbreaks that could threaten the United States. Furthermore, a robust surveillance system will serve to deter terrorist use of biological weapons, as early detection will help mitigate the intended effects of such malevolent uses.

The purposes of this Act included:

To enhance the capability and cooperation of the international community, including the World Health Organization and individual countries, through enhanced pathogen surveillance and appropriate data sharing, to detect, identify, and contain infectious disease outbreaks, whether the cause of those outbreaks is intentional human action or natural in origin;

and

to provide assistance to developing countries to purchase appropriate communications equipment and information technology, including, as appropriate, relevant computer equipment, Internet connectivity mechanisms, and telephone-based applications to effectively gather, analyze, and transmit public health information for infectious disease surveillance and diagnosis.

On the positive side, both Bills should provide additional information to the mission areas of homeland security. S 871 in particular has an additional strategic value, beyond homeland security, which is national security. The support of a global pathogen network worldwide can help prevent irreversible damage inside and out of the United States. On the negative side, many U.S. citizens could fear breaches of their privacy in the case of S 1230. For example, imagine a U.S patient with (HIV or) AIDS. If a physician would provide that information to a public health department and then it was given to DHS with geographical coordinates, people (besides the healthcare providers) would know the precise location of that individual. If that information reaches the wrong people, this individual could be discriminated against.

Parallel Paths for Crisis/Emergency Management and Management of Terrorist Threats

The preparation, response, recovery, and management of an emergency/crisis [17] regardless of what caused it, i.e., a human and/or machine error, a natural catastrophe or a terrorist attack, is pretty much the same in all cases. Of course, different agencies get involved in addition to emergency preparedness and response personnel in a terrorism scenario than during an earthquake.

If we consider then a nuclear reactor, a hydroelectric dam, a gasoline "statewide" pipeline system, or an electric power station, all of these systems for example rely on the use of computers and communications systems for everyday activities including systems control. Although an operator of any of these systems could make a mistake or the systems themselves may fail, redundancies are built in so that alternative paths are available for a continuation of services. The identical paths that are triggered when a crisis occurs allow for the planning, preparing, managing, and recovering from the mistake. Modeling and simulation offer tools that allow for the creation of different scenarios and the practice of crisis management. From the stages of identifying vulnerabilities and threats, to risk assessment and consequence management, these processes require most of the same resources regardless of its causes. The same could be said for the need of "continuity of services." For example, if a water dam provides both drinking water and electricity to the population and an earthquake damaged these facilities, not only is it important to restore the services while fixing the damages, but contingency plans are needed so that immediately the essential services of delivering the drinking water and providing electricity can be restored.

Threat and Risk Management

According to a GAO report [18], two key issues (out of six) for homeland security are: "utilizing threat and risk management to estimate character, probability and impact of attacks" and "identifying desirable or attainable levels of risk prevention, vulnerability and recovery response." It is important for our readers to reflect that the words "threat" and "vulnerability" will have different meanings to each of the first responders, i.e., each of the profession that they exercise. A policeman; a firefighter; a public health official; a soldier; a security person from a nuclear reactor, a gas pipeline, a hydroelectric dam or any of the transportation mechanisms (air, land, or sea) each has their own definition of the word "threat," which is accompanied by their own set of vulnerabilities. The range of meanings for the term "threat" then is very wide; i.e., let's assume for those professionals named above (respectively) the following events: a crime, a fire, the spread of a virus and/or bacteria, the enemy, a nuclear-plant accident, a breakage in a gas pipeline, a blackout and/or a flood, an airplane crash or a train derailment or the sinking of a ship. For each of these threats there are a number of vulnerabilities that need to be identified by those professionals. These risk and vulnerabilities assessments allow for contingency plans and for crisis and consequence management planning. In addition it allows those in charge of asset protection to determine what resources are needed, and given the resources they have (prioritization), where they need to go. One area that all the above professionals share is with the use of information systems. Questions that they all need to answer while assessing risks include: what is at risk? What are the consequences according to the size of the threat? What interrelations affect other systems? In other words, the threat and risk assessment starts by identifying assets and weighing how sensitive each one may be. Threat analysis will then identify (threats) and assess what is compromised and its consequences. Risk analysis will identify vulnerabilities, and the required safeguards, and assess risk. Many assets cannot be assessed just as such but rather as a component of a larger picture. This is why studying the interrelations among certain assets (i.e., systems, infrastructures, etc.) and using a systems approach is a fundamental must when we do this process.

In October 2003 as hurricane Danielle swept the Washington, DC, area a blackout followed for several days.
Citizens would be able at the local and individual level to deal with the blackout as in many other instances in the past. What is different now in 2003 with respect to the healthcare system (compared to the one of a few decades ago) is that:

(a) Patients are being discharged earlier than in the past from hospitals. [Usually this process is explained as: saving healthcare costs to health maintenance organizations (HMOs), minimizing hospital related infections, reducing possibilities for medical errors (i.e., According to the IOM report: “To Err is Human” [19], about 98,000 Americans die every year from medical errors), and improving outcomes, i.e., faster recovery, better quality of life, etc., by having the possibility of being with relatives and/or in a familiar environment.]

(b) The option of homecare via telemedicine and/or disease management via the Internet has taken off. This new growing environment shows: 1) A very large (105 million Americans, including the elder) population with chronic diseases started to use the homecare option; 2) patients using at times respirators and/or ventilators and/or ECG equipment while recovering from surgery at home; 3) healthcare practitioners doing patient management through the Internet (to the patient’s home); and 4) special medications being kept refrigerated in these homes. Although nobody questions the criticality of a hospital’s need for a constant availability of electrical power, perhaps we need to revise what is the critical infrastructure in the year 2003 and beyond timeframe and what should be done about it. For example, in the future houses may come with mechanisms that include emergency power generators so that citizens would be able at the local and individual level to deal with such emergencies until services are restored. Should this type of requirement be advised for future home construction blueprints? Let us not forget that when we purchased a home, for example, 30 years ago, nobody would looked to see if a room had light switches, electric outlets, and a telephone line connection. A house would ordinarily have a single place for a telephone line and every room would have both electric switches and outlets. Slowly telephone lines jacks started to appear in every room of the house, and the need to combine both voice and data communications for single-family homes became a reality in the late 1990s. It is not uncommon these days to purchase a home that already includes a local area network, and the availability of DSL is the norm in most U.S. metropolitan areas. In addition, television access is not just via a “regular antenna” anymore, but cable and special dishes/satellites offer new services that include access to the Internet and associated services on demand. For these purposes, many TV sets come equipped with adapters for keyboards that allow for easy interaction with specific services (both types: free or fee for service).

The Role of Information Technology

Despite all the sophisticated technologies that surround us these days, all it took was the smartness of an alert family practitioner in Florida to discover the Anthrax threat (late 2001). In our current “developed” society, IT plays a very key and central role that pretty much defines and dictates the way we live. The way we work, learn, play, shop/purchase, communicate with others, plan activities, manage our health, read/listen to the news, and store and retrieve information (our own and others”) is greatly influenced by whatever systems (i.e., system and application software and hardware) we may have available. Technology by itself will not solve our problems, either. Currently, finding people with the right knowledge and training is perhaps an even more difficult task to achieve.

Knowledge Management

According to Fensel [20], the Web currently contains around 3 billion static documents, which are accessed by over 500 million users internationally. At the same time, this enormous amount of data has made it increasingly difficult to find access and present and maintain relevant information. This is because information content is presented primarily in natural language. Thus a wide gap has emerged between the information available for tools aimed at addressing these problems and the information maintained in human-readable form. The uses of data mining can be multiple and offer timely information that can not only save many lives but also improve the quality of our lives. For example, the Food and Drug Administration (FDA) announced [21] the establishment of a Cooperative Research and Development Agreement (CRADA) with Lincoln Technologies, Inc., to use data mining and enhance FDA’s ability to monitor the safety of drugs, biologics, and vaccines after they have been approved for use. (Note from a privacy point of view that the specific data set used for data mining purposes does not include patient names, addresses, social security numbers, or similar information.) Data collected from suspected drug-related adverse event reports and other electronic medical information could aid the FDA in identifying “signals” of adverse events and the patterns in which they occur. The more effectively the tools FDA can use to detect such patterns, the faster it can act to evaluate and act...
on these reports as appropriate. For example, more effective data mining might allow the agency to identify a pattern of adverse events in a specific population of patients taking a drug/vaccine, or in patients who take a certain combination of drugs/vaccines, and the agency could then communicate this knowledge sooner to medical professionals and patients—preventing more adverse events.

Sizing the “Information Glut” and ... the Data Sharing Imperative

IT has become an intrinsic part of our lives, and the price-performance of these systems has made the complexity of sharing content a bigger issue that it was two decades ago when the first PC was announced. Not only do the numbers of people using IT keep increasing, but as processor speeds and storage capacity keep going up, the magnitude of data stored keeps increasing exponentially. In order to protect critical infrastructures we need to cross public, private, and even individual boundaries. In other words, information may need to flow from home (individual) to a hospital (private) and a fire department (community/public) and vice-versa.

To help illustrate the magnitude of this problem, let us reflect, for example, on the first IBM-PC, which was announced in 1980 without a hard drive. The first hard-drive offered had a capacity of 10 MB. Off course, today for less than US$1,000 we can purchase a system with 60–80 GB of storage capacity. If we would use the system exclusively to store text, and we assume 1-byte characters (1 byte = 8 bits) and 3,500 characters per page, this would translate into 17 to 22 million pages of information. From a content point of view, these pages would be in proprietary binary formats that cannot be searched as plain text. According to Daconta [22], when we scale this example up to corporations we see both the storage capacity and diversity of information formats and access methods increase ten- to a hundredfold multiplied by the number of employees. It is becoming very clear the increasing complexity that we will be facing just to do knowledge discovery. When we add the issue of timeliness for the knowledge discovery in order to prevent, for example, a terrorist attempt, the message becomes very clear: we need to change our methods, our systems, our infostructures, our procedures, and our policies.

Fig. 3. The landscape for intelligence sharing among first- and second-tier responders. From (23) by permission of Innovative Technology Systems (ITS) and Lockheed Martin SMDS and the presenter.
In the intelligence and warning mission area we find a very complex “landscape” as presented by Dr. Ayen [23] when intelligence data needs to be shared among first- and second-tier responders. As we can see in Figure 3, the information may be crucial to prevent and/or interdict an attack. The information may come from a very large number of sources, i.e., intelligence agencies, civil agencies, and law enforcement; international agencies and foreign governments; and private industry. The actual risks/threats may be not only for “critical infrastructures” but a wide array of stakeholders that includes private citizens and private industry and local, state, and federal governments. The challenges are many and include not only security of data and network communications but doctrine, policy, methodologies, tools, and processes that need to be practically integrated with an extensive number of “content” expertise [24]. For example, each of the risks (areas that appear on the top of the figure), i.e., biological, chemical, nuclear/radiation or cyber terrorism, requires a different type of expertise. Of course, we could make this landscape even larger by adding, for example, other risks such as food, air, and water, etc.

Associated Impact of Cyberthreats
In many instances, threats that seem strictly cyber, because of our IT dependencies (within all of our “business processes”) and the IT interrelations within all critical infrastructures, may cause both quantitative and qualitative damages that go beyond our expectations. For instance, Kun [25] reported that on 7 May 2000 the “I love you” virus contaminated over 1 million computers in five hours and closed the Centers for Disease Control and Prevention (CDC) computer system for six days. It was since estimated that the virus, while sweeping the globe, infected approximately 60 million computers causing damages of US$ 13 billion. In addition the virus’ author, a Filipino computer science student, escaped prosecution because the Philippines have no computer crime laws. I believe that currently it is a basic necessity for all nations to work together in resolving the “jurisdictional-cyber-issues” since crimes of this nature can be done remotely from anywhere to anywhere else.

From a lessons-learned point of view, it needs to be remembered not only the damages caused by these types of events but the need for a total threat and risk assessment plan of a (potential) crisis occurring just at that particular moment (that a cyberthreat occurs) and regardless if it is caused by accident or by design. In the last example, what if we had a bioterrorist attack during the period (six days) when the CDC’s computers and communications were down? How would a local or state health department (LHD or SHD) be able to access the Web-published epidemiological clinical (prevention guidelines) information published by the CDC’s Epidemiology Program Office (EPO)? What are the plans and redundancies required to assure a continuance of the “business as usual” process?

An interesting scheme was presented by Symantec’s Liebenstein [26] (see Figure 4) regarding the steady increase of detected software vulnerabilities (indicating the trend they are seeing relative to software vulnerabilities—flaws in the software that can allow an intruder or malicious code to gain unauthorized access) from ten a week in 1999 to 60 a week in 2003. Attacks are becoming faster and more aggressive. In the first half of 2003, they saw more attacks that focused on new vulnerabilities. For example, 64% of the attacks targeted vulnerabilities less than a year old; 66% of the attacks targeted vulnerabilities that were rated “highly severe.” In addition, we’ve seen signs that the vulnerability threat window—the time between when the vulnerability becomes known and when an exploit begins to spread—is shrinking. Blaster, for instance, spread only 26 days after the vulnerability was first announced. By comparison, the data shows that most vulnerabilities are typically exploited about six months after they’re discovered. Symantec also reported a dramatic increase of 123% in viruses and worms compared to the first half of 2002. They have also seen a significant increase in malicious code that targets instant-messaging (IM) clients and peer-to-peer networks (P2P) (400% increase in viruses and worms that use IM and P2P as a spreading mechanism).

![Early Warning for the Blaster Worm](image)

**Fig. 4.** Early warning data of Blaster worm compiled by Symantec DeepSight Threat Management System. From (26), by permission of the author.
attacks are targeting new vulnerabilities, new vulnerabilities are being exploited more quickly, and faster exploitation requires better patch management policies. Staying on top of alerts, updates, and patches is such that most business and or individuals are not being able to do it. The use of electronic warning systems (see Figure 4) such as Symantec™ DeepSight™ Threat Management System (TMS) (which is a global early warning system for attacks that utilizes expert threat analysis, assessment, and decision support) is one of the recommended mechanisms to deal with this type of activity.

The following example shows that information alone will not solve the problem; procedures need to be in place and need to be strictly followed and enforced. In January 2003, a self-propagating worm called Slammer showed the vulnerability of systems and the problem of not using available protective measures. There was a known flaw on Microsoft’s structured query language (SQL) database that could be corrected with an available patch. The negligence of many systems administrators, who failed to update their systems (not having the patch installed in their systems), caused thousands of systems to get infected and a complete disruption of their networks. The information and communications sector (I&C) took a huge hit on 11 September 2001, both in human terms and physical destruction. Many I&C professionals died in the attacks and much of the destruction consisted of property, including computers, software, and data. One estimate places losses in IT resources by the financial community alone at US$3.2 billion. Morgan Stanley estimates losses of IT hardware, restoration of services, long-term IT costs to enterprises, and annual World Trade Center IT spending at over US$25 billion [27].

It has been said in multiple occasions (by the Secretary of DHS) that 85% of the Critical Infrastructure, both physical and cyber, belong to the private sector. It is imperative then that the coordination for protection purposes in particular will require a very close communication between the private sector that owns these infrastructures, the local authorities (i.e., local, state, regional, in which these infrastructures reside), and the federal government, which has the responsibility for its protection.

Securing Cyberspace

Our Nation’s critical infrastructures [28] are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. This National Strategy to Secure Cyberspace is part of our overall effort to protect the Nation. It is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people. [29]

New Division at DHS

The Department of Homeland Security created a new division to address threats to the nation’s technological infrastructure [30]. Called the National Cyber Security Division (NCSD), the unit is charged with addressing potential security breaches to private-sector and government computer systems and was created as part of the National Strategy to Secure Cyberspace [31] and the Homeland Security Act of 2002 [32], and it will be run under the Department’s Information Analysis and Infrastructure Protection Directorate. Because of interdependencies it is becoming increasingly difficult to separate cyber operations from the physical aspects of business programs. This new division will be focused on the vitally important task of protecting the nation’s cyber assets so that we may best protect the nation’s critical infrastructure assets. Areas that this division will be working on include: identifying risks and reduce vulnerabilities to government and private-sector computer systems; operating a Cyber Security Tracking, Analysis and Response Center to detect attacks to the Internet and alert the public; and developing education programs on security measures. The existing capabilities from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System will all be part of NCSD’s foundation.

Privacy and Security or Privacy Versus Security

The intelligence and warning mission area of homeland security is perhaps the most fundamental one to prevent an attack or if unavoidable at least to warn us of it and reduce our losses. Yet every time we read an article that may suggest a tool and/or technique, the conflict with the right to privacy surfaces. Here are three examples:

1) The State Department (SD) plans to develop “intelligent” passports [33] that will carry facial images with biometric data
on advanced computer chips. While the SD plans to use facial recognition, the Homeland Security Department’s entry-exit biometrics system will store two fingerprint images and a digital photograph of visitors to the United States in databases at consular offices and points of entry nationwide.

2) The Defense Department developed a worldwide radio-frequency ID network to track tagged cargo from its origin through the transportation system to its final destination [34]. “In 1991, there were thousands of cargo containers flooding the ports of Southeast Asia, because of the difficulty of matching paper manifests with shipping containers tens of thousands of containers had to be opened to find out what they held, and a lot of time and material were wasted. According to the General Accounting Office, US$2.7 billion worth of spare parts shipped to the Gulf theater in 1991 went unused. The use of this technology would prevent such a recurrence.

3) In the private sector—Wal-Mart Stores Inc. [35] recently announced plans to require its suppliers to use RFID (radio-frequency identification) tags. An RFID tag on a pallet of merchandise makes it possible to track inventory by storing information on a tiny tag that can be read remotely via radio signals.

Although the technologies in all three of these cases could help us be better protected, save billions of dollars, and/or become more productive, the issue of privacy will without any doubt generate anxiety among those fearful of breaches to their privacy. A balance is clearly needed and recommended, but in addition multiple use of the technology will facilitate its adoption. For example, the use of biometrics is mostly associated with authenticity issues related to security. What if we use it for the purpose of helping prevent medical errors in patients while they are in a hospital environment (i.e., 98,000 Americans die every year from medical errors)?

**Semantics and Vocabulary in Homeland Security**

Multiple types of threats can affect the public health (i.e., air, water, food, biological, chemical, nuclear/radiological, cyber, etc.) Presently in this magazine in the September/October 2003 issue [36], different terrorist threats to the public health are being addressed by different agencies, i.e., CDC/NIH (biological, chemical, etc.), EPA (water, air, etc.), DOE (nuclear, radiological, etc.), USDA (livestock, plants/food, etc.), DOC/HLS (cyber security), etc. Last year the author [37] suggested the alternative of having multiple lanes in the same highway where each agency/department would address public health from their respective area of expertise instead of multiple redundant highways built by each agency/department. In May 2003 the CDC introduced the Public Health Information Network (PHIN) [38], which is precisely what was recommended to address this need.

Now the issue becomes the use of the “right vocabulary.” Not only does each agency has its own semantic/vocabulary, but when trying to create a unified PHIN, these vocabularies need to be “adjusted and/or translated” depending on the analyst/reader is someone, for example, from the Department of Health and Human Services or the Department of Homeland Security. “Semantics and Vocabulary in Homeland Security” [39] was presented in September 2002 during a special one-day conference on the Semantic Web at the White House Conference Center. Of particular interest was to determine how analysts doing intelligence work (with no background necessarily on public health (i.e., environmental, biological, chemical, nuclear/radiological and/or cyber threats)) may be able to look at data from multiple agencies and do the correct interpretation of what they are analyzing. Earlier in this article, “intelligence and warning” was described as one of the mission areas of the National Strategy for Homeland Security. Since homeland security and/or public health require the integration of information from multiple stakeholders and the use of different vocabularies occurs (among the different agencies, departments, private industries, etc.), the meaning obtained may not be the corresponding one. How can semantic technologies help resolve the issue of interpretation of the integrated information, depending on who the stakeholder analyzing it may be, or realizing who the source is and what was the “true” meaning of a message?

**Background**

According to the American Heritage Dictionary of the English Language [40] a coronary care unit (CCU) is:

- NOUN: abbr. CCU A hospital unit that is specially equipped to treat patients with serious heart conditions, such as coronary thrombosis.

and in the Merriam-Webster’s Medical Dictionary [41] the CCU abbreviation means:

1) cardiac care unit
2) coronary care unit
3) critical care unit.

In the fall of 1978, fresh out of my engineering doctoral program at UCLA, I went to work for IBM. I recall that two of my first observations on the job were: (a) The number of acronyms used in the (U.S.) “business” community, and (b) the variance on the meanings that those acronyms had depending (particularly) on who was speaking; i.e., their area of specialization and/or expertise. One day, while working at my desk a discussion started where my neighbors were discussing a problem with the CCU at the Los Angeles County Medical Center account. Of course, as a biomedical engineer I believed they spoke of the coronary or critical care unit every time I heard that acronym. After a few sentences the conversation was not making any sense. So I thought I was probably not hearing well or I must have missed something. Shortly after I asked what were they talking about and I learned that the CCU was the Communications Control Unit. Let’s now move forward to the year 2003 and do a search for “CCU” on the World Wide Web (WWW). Is it a coronary care unit/cardiac care unit or a communications control unit? ... hardly. A thousand results later I stopped looking. The results covered a spectrum of fields including: stock/financial market, credit unions, educational, armed forces (i.e., army, navy), crime units, medical (i.e., disease related, unit related), sports, technology (i.e., computer related, communications related, camera related, etc.), religious organizations, pornography, beer producers, airports, etc. In addition, language becomes an issue when using search engines on the WWW. Unless special filters are used, the search engines go and get information regardless what the source is or where it is from. This effect increased considerably the number of hits. See Table 2 for some of the results.

For example, by creating subcategories in terms of the “application” areas/“industries” (i.e., technology, health, financial, sports, religious) filters could help reduce the num-
ber of “hits” that would appear while doing a search. In other words, the results could be divided by subcategories. This methodology would not be sufficient to resolve the issue. The creation of a multiple set of vocabularies/translation tables will become increasingly important for all homeland security mission areas. Let us not forget that the information we may be looking for may exist in some place and may not be written in English. Since “machine translation” is not the same as “cultural translation” this task at hand is not trivial. The tagging of information is also an imperative so that we can facilitate the discovery of information. More details on this topic (i.e., tagging of information, XML, etc.) can be found in this issue in N. Guzman’s article.

The Global Village’s Critical Infrastructure—Cyberinformation and Public Health

On the IT side, despite two years of effort, formidable hurdles still affect information exchange between first responders at the local level, members of a panel told the Industry Advisory Council’s Executive Leadership Conference in October 2003 [42]. According to Steve Cooper, chief information officer at the Homeland Security Department: “The sector that’s the farthest along in information sharing is law enforcement,” and “The sector that appears to be the least well-integrated is public health.”

Today we can virtually visit any country and get information from anywhere in the world in a matter of seconds. In addition, fast modes of transportation have closed the physical distances that existed just a century ago. The possibility for disease to travel along with us by accident or by design is a reality. These types of threats and our related vulnerabilities need to be looked at very closely and addressed as soon as possible. Public health presents a picture for homeland security that is not as easy to control or delineate as a physical structure is, i.e., a bridge, a power plant, or a building. A fixed location, for example, is easier to protect. Public health has certain similarities to a cyber threat. The same way a computer system may be “infected” and waiting for a specific day, and/or time, and/or circumstance to be activated, a pathogen may be inside a human (or an animal’s) body incubating, and since no symptoms or signs are manifested, it may be assumed that everything is okay. In many cases, even if certain symptoms are observed, it is almost impossible to determine what it represents. For example, flu-like symptoms are observed in individuals exposed to both anthrax and Severe Acute Respiratory Syndrome (SARS). This makes the task of people at our borders practically useless for biological-related detection. Also the concept of “inside” versus “outside” our borders is useless when it comes to health threats. In 2003 alone the United States had four situations, West Nile Virus, monkey pox, SARS and mad cow disease, that showed how rapidly a disease can spread through the globe. As seen in the data in Figure 5, it is evident the very short timeline for the occurrences and for the global spread of SARS.

Geberding [43] showed that the first case (A) from Guangdong Province, China, (see Figures 6 and 7) and two hotel guests who became ill (cases H and J) started outbreaks of SARS in three Hong Kong hospitals involving at least 95 healthcare workers and more than 100 contacts. Case B flew to Hanoi, Vietnam, was hospitalized there, and started an outbreak among healthcare workers and their contacts. Cases C, D, and E returned to their home in Singapore and started an outbreak there. Cases I, L, M went to the U.S., and Case K went to Ireland. Cases F and G started an outbreak focused in Toronto, Canada.

The key points of these events were: 1) the seriousness of the illness requiring hospitalization, and ICU, sometimes leading to death; 2) the high proportion of healthcare workers among the cases; and 3) the rapid international spread. Also, while most of these early recognized clusters suggest that contact and droplet transmission are predominant, the pattern of transmission in the hotel suggests the possibility of airborne or fomite transmission (fomite is an inanimate object or substance, such as clothing, furniture, or soap, that is capable of transmitting infectious organisms from one individual to another).

Some consequences and impact: beyond the generated public fears, hundreds and thousands of travelers avoided (and may still avoid) places like China, Taiwan, Hong Kong, Vietnam, Singapore, and Toronto. The women’s World Cup soccer tournament was cancelled in China in 2003. Because of mad cow disease the import of U.S. beef products was stopped by many countries including Japan, Korea, Taiwan, and Canada. It is too early to calculate the long-term “fear-effect” on the U.S. population’s consumption of beef and the related economic consequences for the U.S. beef industry. The magnitude of these economic “disasters” is such that they can make you wonder, however: “what if they were not Nature’s accidents but rather “man-made?” After September 11 it is not
Table 2. Some results from searching the acronym “CCU” on the World Wide Web.

1. Clear Channel Communications (NYSE; last trade 8/7: 38.25)
2. Colorado Christian University (http://www.ccu.edu/)
3. Consultative Committee for Units (France) Measurements Database (www.bipm.fr/enus/2_Committees/CCU.shtml)
5. Chung Cheng University (National University in Taiwan, http://www.ccu.edu.tw/)
6. Compañía Cerveceras Unidas (Chile) (http://www.ccu-sa.com/)
7. Centre Culturel d’Uccle (Belgium) (http://www.ccu.be/)
8. Universidad Michoacana de San Nicolas de Hidalgo (Mexico) (http://www.ccu.umich.mx/)
9. Component Conversion Utility (html, xml, java, java, script, sql, etc.): (http://www.jshift.com/products/ccu/)
12. Canadian Unity Council (Canada) (http://www.ccu-cuc.ca/)
14. CC United/CCU Academy, etc. (Soccer Programs): (http://www.ccuprograms.com/)
15. Military—Naval Brig/Correctional Custody Unit Puget Sound (http://www.brigpuget.navy.mil/)
17. Columbia Credit Union (Canada) (http://www.columbiacu.org/aboutccu.html)
18. Capitol Credit Union (http://www.ccu.rox.org/info/about.html)
19. Central Credit Union (http://centra.org/about/default.asp)
20. Campus Credit Union (http://www.campuscu.org/directory.html)
21. CC Unlimited (Check Republic, information and communications technologies) (http://www.ccuni.com/)
22. X-rated site.
23. Croatian Catholic Union of the US (http://www.ccu-usa-can.org/)
24. Medical—Crohn’s og Colitis Ulcerosa (Island) (http://www.doktor.is/ccu/)
26. Campionats de Catalunya Universitaris (Spain) (http://www.upf.es/ecu/normgen.htm)
27. Charlotte County Utilities (Florida) (http://www.charlottecountyfl.com/CCU/)
28. Constitutional Court of Ukraine (Ukraine) (http://www.ccu.gov.ua/pls/wccu/indx)
32. Central Computing Unix System (Canada) (http://www.umanitoba.ca/campus/acn/unix/)
33. Circumpolar Conservation Union (http://www.circumpolar.org/index.htm)
35. Channel Coding Unit (The CCU is a redundant Channel Coding Unit for encoded fast data transmission) (http://www.ohb-system.de/SpaceTech/Electronics/ccu.html)
36. Commissione Consigliare Urbanistica (Italy) (http://www.provincia.ps.it/urbanistica/2-urbanistica/2-2_home.htm)
37. Charge Control Unit (CCU) presents an attractive alternative to the more traditional methods of charging spacecraft batteries (http://www.spectrumastro.com/ProgramsProducts/CCU.asp)
38. Correspondence Control Unit (CCU) Department of Education: (Within the Office of the Assistant Secretary for Special Education and Rehabilitation Services, the CCU controls correspondence, documents receipt of all mail addressed to the Assistant Secretary)
39. Cyber Comp Union (Canada) (http://www.sfu.ca/~ccu/)
41. Cow-Calf Teaching and Research Unit (http://ars.sdstate.edu/facilities/ccu/)
42. Console Control Unit (http://www.organworks.com/cat/cow_8tv9.htm)
43. Communications Control Unit (GERMANY) (http://www.telefunken-sendersysteme.de/Produkte/UKW_Sender/ZBG_7456.pdf)
44. Central Coordination Unit (http://www.cites.org/eng/news/vacancy/mike_data_coordinator.pdf)
45. Coastal Carolina University
46. Confederation of Canadian Unions (Canada) (http://www.ppwc.bc.ca/ccu.html)
47. Cockpit Control Display Unit (CCU) (http://www.interfacedisplays.com/hiddocs/NewFiles/CCU.pdf)
48. Calcutta Airport (CCU) (India) http://www.ciaa.co.uk/Calcutta_Airport_CCU_5170848
49. Corporate Citizenship Unit (CCU) (United Kingdom) http://www.wbs.ac.uk/expertise/research_teaching/ccu.cfm
50. Cell Culture Unit (CCU) is being developed for use on the International Space Station. http://brp.arc.nasa.gov/GBL/Habitats/ccu.html
hard to imagine individuals, i.e., from terrorist groups, organizing and planning for such situations with the purpose of generating great fear, great disruption, and great economic losses. What is also becoming clear to many is that no matter the causes of the public health crisis (i.e., disease) or where it may occur, the need for fast and accurate information is the most important ally for containing it and/or defeating it.

Using the SARS events of 2003 as an example, Kun [44] demonstrated the need for sharing surveillance and epidemiological information worldwide and in real time. He also showed the need for using data standards, geographical information systems (GISs), geo-coded information, and even the use of handheld devices to input data with embedded spatial information from areas where the need for recording geographical coordinates is a must, (i.e., places where a dead animal/insect may be found for certain diseases). The use of a global partnership is essential in obtaining the right information at the right time. Communications mechanisms such as the Internet are facilitating this task, but they are not enough.

His message became the foundation for the Italian sponsored (European) GeoSARS (Georeferenced Surveillance of Acute Respiratory Syndromes) project. The two key partners: INFORMA an Italian service company operating in the medical-scientific sector (clinical and pharmaceutical research) and the Italian National Institute for Infectious Diseases “Lazzaro Spallanzani”—the leading National Italian institution for research and care of infectious diseases [45]—have been recently collaborating to the definition of the GeoSARS project. They aim to develop an information system, integrated with geographic referencing technology, to support public health officials in syndromic surveillance activities (i.e., the monitoring of the frequency of illnesses with a specified set of clinical features in a given population) in the field of acute respiratory syndromes. It will enable public health officials to store and process all relevant clinical events reported by a number of emergency rooms distributed in the region under surveillance. The GEOSARS-IS will provide support for cluster detection by implementing automatic alarm mechanisms, triggered by the concurrence of prespecified sets of discriminating features, whose definition will be dynamically adaptable to changing epidemic scenarios. GPS will be initially
used as a de facto standard for satellite global positioning, even though the system architecture will be designed with an eye to the results of the pan-European Galileo initiative. A prototypical European GeoSARS network will be realized, comprising initially three nodes deployed in important European health institutions, which will actively participate in the definition of system requirements and in the piloting phase, thus establishing the project’s peculiar scientific research objectives. Virtual private networks will be implemented to link the nodes to each other and, at node level, each of the public health institutions with the emergency rooms involved in the system piloting.

**Conclusion**

An interesting phenomena is that the use of different weapons of mass destruction would produce actions that are diametrically opposite in order to achieve positive outcomes. For example a biological threat like smallpox/monkey pox or SARS, which are highly contagious, require complete isolation of those exposed (both patients and caregivers); on the other hand, the explosion of a nuclear or hazardous chemical plant would require an immediate evacuation of thousands of individuals. These evacuations may be immediate or could linger, i.e., occur many years later, and could extend from small to fairly large areas. For example, a *Washington Post* [46] article reported in 1990 that Soviet authorities, realizing they underestimated the extent of the Chernobyl accident, had to evacuate 14,000 more people that year from the site and that more work was needed to limit the damage from the 26 April 1986 explosion and fire at the nuclear power reactor that, according to official figures, killed 31 people. The article quoted that already 90,000 people had been moved from their homes in the years following the accident, apparently in addition to the 100,000 taken out of the 20-mile zone a few days after the disaster.

Most local, state [47], and federal agencies/departments are to an extent “islands of excellence.” The silo approach that many of them have pursued for decades makes the homeland security tasks of today, i.e., sharing information among interoperable systems, more difficult to implement [48]. This scenario is unfortunate since the complexity of interdependent systems demands the use of modeling and simulation to create an overall strategy as framed in [2]. Haimes offered a picture on how systems engineering techniques can help design, develop, and deploy (see Figure 8) a framework for homeland security. The needed strategic plan will surface by looking at those four risks (human lives, individual property, etc.; economic structures; critical cyber-physical infrastructures; orga-

---

**Fig. 7.** Spread of SARS, spring 2003. From [43].
The interrelations go beyond the technical aspects, though. While reviewing homeland security and public health policies it has become apparent that interrelations among multiple policies exist (see earlier section on policy analysis and rational). This conclusion requires then that we use the systems approach both for technical as well as policy for the purposes of creating effective and efficient processes that are not partial on one hand nor redundant on the other in their implementations and/or considerations.

Acknowledgments
The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.

Luis Kun is currently a professor of systems management at the IRM College of the National Defense University, where he is the course manager for Homeland Security; Intelligent Agents and Decision Support Systems. Prior to this, he held several senior-level positions in industry and government. He was the director of medical systems technology and strategic planning at Cedars-Sinai Medical Center in L.A.; the senior IT advisor to the Agency for Health Care Policy and Research where he formulated the IT vision and was the lead staff for HPCC program and Telehealth. He coauthored the Reports to the Congress on Telemedicine (1997) and on HIPAA Security. In July of 1997, he was an invited speaker to the White House. He was largely responsible for the Telemedicine portion of the bill that became part of the Balanced Budget Act of 1997.

Dr. Kun represented the DHHS Secretary at a Pan American Forum of Health Care Ministers on Telecommunications and the Health Care Industry in Mexico in 1997. As a Distinguished Fellow at the CDC (1999–2001) he was the Senior Computer Scientist for the Health Alert Network for Bioterrorism and later the Acting Chief Information Technology Officer for the National Immunization Program (NIP), where he formulated their IT vision.

He was an expert witness to Congress on the area of HPCC and the IEEE Health Care Engineering Policy Committee Chairman of the Electronic Medical Record and High Performance Computers and Communications Subcommittee. He served as the conference chairman of the Health Care Information Infrastructure (HCII) conference in 1995. Dr. Kun holds B.S.E.E., M.S.E.E., and Ph.D. degrees in biomedical engineering, all from UCLA. Dr. Kun has

made numerous seminal contributions to the information technology discipline. In March of 2003, he received the 2002 IEEE-USA Citation of Honor Award “for exemplary contributions in the inception and implementation of a health care information technology vision in the United States.” Dr. Kun currently serves as chairman of the Bioterrorism & Homeland Security Working Group for the IEEE-USA Medical Technology Policy Committee. Dr. Kun is a Fellow of the American Institute of Medical and Biological Engineering (AIMBE), where he serves as chairman of the Bioterrorism R&D SWAT (Strategic Working AIMBE Team).

In the past 25 years Dr. Kun has written many articles and book chapters/sections, and he is currently the editor in chief of the Handbook of Biomedical Information Technology for Elsevier. He has lectured on medical and public health informatics, information technology, and biomedical engineering in over 50 countries. He is in the IEEE Computer Science Distinguished Visitor Program for both the U.S. and Latin America (2003–2006) and is/was on the advisory board of many magazines and professional journals. He has served as an invited chair of conference, tracks, sessions, tutorials, special symposia, and/or publications and as invited speaker/keynote speaker in conference scientific committees over 150 times.

Address for Correspondence: Dr. Luis Kun, IRM College - National Defense University, Fort McNair, Washington, DC 20319. Tel: +1 202 685 2786. Fax: +1 202 685 3974. E-mail: 1.kun@ieee.org.

References