COMMON DEFENSE AGAINST UNCOMMON THREATS:

THE FEDERAL ROLE IN CRITICAL INFRASTRUCTURE PROTECTION

Report of the
President's Commission
on Critical Infrastructure Protection

1997

Acknowledgment

The Commission gratefully acknowledges the singular leadership and important contributions to the development of this report made by Colonel James H. Kurtz, United States Army, while serving as the Commission's Chief of Staff. This document provided important insights into understanding the concepts of modern warfare, and how our Nation can begin to think about infrastructure threats in new and creative ways, while drawing upon the considerable wisdom and lessons of history.

CONTENTS

Common Defense Against Uncommon Threats:

The Federal Role in Critical Infrastructure Protection

"Protecting the security of our nation – our people, our territory and our way of life – is my foremost mission and constitutional duty."

-- President William J. Clinton[1]

The notion of infrastructures as targets is not new. Clausewitz wrote that in war, one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics, he said, a certain *center of gravity* develops, the hub of all power and movement, on which everything depends. For a nation seeking victory in war, the enemy's center of gravity is the point against which all energies should be directed.[2] Infrastructures are a dominant characteristic of developed nations, high on the list of potential centers of gravity to be considered for attack by an enemy.

For the first 175 years of our existence as a nation, from 1775 until about 1950, geography protected our national infrastructures. They could be attacked only by an invading force, as in the War of 1812, or from within, as during the Civil War. Until the advent of long-range bombers and intercontinental ballistic missiles, the US was never faced with a hostile power that had the military capability to seriously threaten our homeland.

Prior to the Cold War, US infrastructures have been all but invulnerable to attack by an invading force. On the few occasions when someone did try to penetrate our borders, they were detected and quickly repelled as shown by the following examples.

- In 1916, Pancho Villa and several hundred followers crossed the border to attack Columbus, New Mexico. They were intercepted by alert troopers of the 13th US Cavalry. Eight US civilians and seven soldiers died in the ensuing gun battle. Two weeks later, General "Black Jack" Pershing led a punitive expedition into Mexico that failed to capture Villa, but defeated and dispersed his followers in a series of engagements.[3]

- In the summer of 1942, German submarines landed two four-man sabotage teams, one near Long Island and the other on the Florida coast. They brought with them enough explosives and incendiaries for a two-year campaign to disrupt US war production. Their specific targets were

aluminum plants, locks on the Ohio River, and rail lines. An alert Coast Guardsman heard the Long Island team speaking German, and they were quickly rounded up. One told the FBI about the Florida team, and within two weeks, before they could do any damage, all eight would-be saboteurs were arrested.[4]

During the Cold War, the physical geography that had protected us from foreign threats was rendered irrelevant by Soviet bombers and intercontinental ballistic missiles (ICBMs). The US developed an extensive early warning capability to compensate for our loss of geographic sanctuary.

Early Warning

After World War II and in the early days of the Cold War, when we enjoyed a nuclear monopoly, our defense policy was one of Massive Retaliation. We publicly stated our intent to use nuclear weapons in the event of an attack by numerically superior conventional Soviet forces against NATO forces in Western Europe. This declared policy deterred Soviet aggression, but when the Soviet Union developed nuclear weapons of its own, and long-range bombers capable of delivering them against the continental United States, the policy of Massive Retaliation gave way to Mutual Assured Destruction.[5] We invested heavily in a system of overlapping radar systems to give us early warning of any Soviet "first strike" attempt to destroy our retaliatory capabilities. The North American Aerospace Defense Command (NORAD) maintained constant surveillance against flight paths from the Soviet Union to Canada and the United States, and commanded interceptor forces whose mission was to defend against an attack by Soviet long-range bombers. When the Soviets developed Intercontinental Ballistic Missiles (ICBMs) and, later, Submarine-Launched Ballistic Missiles (SLBMs) able to reach targets in the United States, we developed overhead sensors. The first were manned high-altitude aircraft, and then satellites whose ocean and other surveillance and sensor capabilities enabled us to keep watch on Soviet missile sites and detect a launch in sufficient time to respond with our own bombers and missiles before Soviet weapons could destroy them. We thus ensured the continued credibility of our deterrent policy of Mutual Assured Destruction. Generations of US political leaders recognized that, in the nuclear world, investments in detection and warning technologies were crucial to our national security.

In the Information Age, however, US leadership cannot count on any advance warning time during which to dissuade a potential adversary or take preemptive action to thwart a cyber attack. Nor is there currently any capability or policy that serves as a credible deterrent to potential attackers.

Cyber Threats to Infrastructures

Cyber capabilities are those that can be used against computer systems in order to shut them down or to gain access to, steal, destroy, corrupt or manipulate computer code and data. Threats to computer systems cover a broad spectrum that ranges from recreational hacking at the low end to organized, synchronized attacks at the high end. However, the basic attack tools – computer, modem, telephone connection and software -- are common across the spectrum. Even at the high end of the information warfare spectrum, the Commission is aware of little in the way of special equipment required to launch attacks on our computer systems.

The Nature of an Organized Attack in the Information Age

If the hardware, software, and skill sets required to conduct cyber attacks are the same across the spectrum from recreational hackers to information warriors, what distinguishes the latter from the former is *organization.* Said another way, an IW attack against US infrastructures may be nothing more than a series of hacker attacks, conducted against carefully chosen and thoroughly reconnoitered targets, and synchronized in time to accomplish specific purposes.

For an organized adversary willing to take greater risks, cyber attacks could be combined with physical attacks against facilities or against human targets in an effort to paralyze or panic large segments of society. These actions could also damage our capability to respond to incidents (by disabling the 911 system or emergency communications, for example), hamper our ability to deploy conventional military forces, or otherwise limit the freedom of action of our national leadership.

As our critical systems become ever more integrated, the potential for an attacker to sow terror and inflict much greater and broader disruption and destruction will grow. At the same time, detecting an attacker and determining whether individual intrusions are part of a concerted attack could become increasingly difficult.

Even horrifying physical attacks such as the bombing of the World Trade Center, the federal building in Oklahoma City, and Centennial Park in Atlanta, produce little physical impact beyond the point of attack. For a physical attack on infrastructures, less spectacular targets could be chosen, such as switching stations, communications antennas, oil and gas pipelines, transformers, pumping stations, and underground cables. Many facilities, whose physical damage or destruction would have a disruptive effect, are located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time to discover the nature of the damage, and in the absence of casualties, it may be some time before the attacks are reported.

The chances of immediately discovering that a concerted cyber attack is underway are even slimmer. Computer intrusions do not announce their presence the way a bomb does. Depending on the skill of the intruder and the technology and training available to their own system administrators, individual companies whose networks are penetrated may or may not detect the intrusions. Intrusions that are discovered may or may not be reported to law enforcement authorities, who may or may not have the resources to investigate them and conclude whether the individual attack is the work of an insider, a hacker, a criminal, or someone truly bent on harming the infrastructure.

In the absence of intrusion detection tools, uniform reporting of incidents as they occur, and some capability to analyze incidents as they are reported, it is conceivable that an orchestrated attack could be under way against US infrastructures for some time before it is recognized as such and the attacker's motives and objectives can be deduced.

Deterrence: Policy and Action

The President's National Security Strategy states that:

> *Our ability to deter potential adversaries in peacetime rests on several factors, particularly our demonstrated will and ability to uphold our security commitments when they are challenged. We have earned this reputation through both our declaratory policy, which clearly communicates costs to potential adversaries, and the credibility of our conventional warfighting capability . . .*[6]

The National Security Strategy defines our *vital interests* as those that are of broad, overriding importance to the survival, safety and vitality of our nation. It declares that we will do whatever it takes to defend these interests, including – when necessary – using our military might unilaterally and decisively. Finally, the Strategy specifies that among these *vital interests* are the physical security of our territory and that of our allies, the safety of our citizens, and our economic well-being.[7] The *physical* security of our territory is a declared vital interest – one we would defend with military force if necessary.

Until a warning capability and related defensive technologies can be developed and fielded, the primary deterrent to potential cyber attackers may be the certain knowledge that the US is committed to an aggressive policy of responding to cyber attacks. A national policy of cyber deterrence should formally define the penalties for nation-states and other entities that attempt to deny or disrupt infrastructure services essential to our national security, economic competitiveness, and quality of life.

This policy of deterrence should consist of several components, including the development of a robust offensive information warfare capability to deliver an overwhelming response in kind; a defensive system for surveillance, assessment and warning of a cyber attack; and a physical strike capability to be used as

a retaliatory mechanism, perhaps for those instances wherein an act of deliberate information warfare results in loss of life or significant property destruction. The foundations for these three components of a cyber-deterrence policy are already in place.

Information Warfare Capabilities

First, our possession of offensive information warfare capabilities was initially demonstrated during Desert Storm, when our military forces successfully took out computerized networks essential to Iraq. This success led to the recognition of our superiority in this area and the continued development and public promulgation of these capabilities should be a critical component of our deterrence policy.

Assessment and Warning Systems

Next, the second component of deterrence should be the development of a defensive system for surveillance, assessment, and warning of a cyber attack. Such a system is essential for providing near real-time notice of an attack in order to protect our own offensive capabilities for a retaliation in kind and to accurately identify the origin of the hostile attack on our infrastructures. However, as electronic communication transport systems allow data streams to flow easily without regard for geographical and political boundaries, technological means alone may not lead us to the origin of the attack with sufficient certainty to decide on a counterattack.

Tracing an attack may involve multiple nations and jurisdictions, most of which are not directly affected by the incident. Efforts should therefore be directed toward negotiating treaties to ensure mutual cooperation at critical times. Some nation-states, whose foreign policies are inimical to US interests, would likely reject our requests for assistance in these matters. Therefore, our deterrence policy should clearly articulate that any perceived hesitation or refusal to comply with tracing attempts may result in a determination that a particular entity is aiding and abetting an information warfare attack against our critical infrastructures, and that such a determination may result in a US counterstrike being targeted against such an entity for the purpose of mitigating the consequences of a recent attack.

Response Policy

Finally, the third component of an effective cyber deterrence policy should be a declaration that any act of deliberate information warfare resulting in loss of life or significant destruction of property will be met with a devastating response. Our precision strike capability and willingness to use it is well established. This policy will clearly establish our intent to use any means at our disposal to protect the security of our nation – our people, our territory and our way of life.

Whose Job is Cyber Defense?

One of the many reasons our Founding Fathers enumerated for establishing the United States was *to provide for the common defense*. The Constitution says that the federal government shall protect every State in the Union against invasion. To provide the means, Congress was empowered to raise and support armies and provide and maintain a Navy.

When the threat to our infrastructures was armed invasion, the US Navy stood in harm's way. When British forces landed on our shores in 1812, the Army and Marines fought them initially and, reinforced by the militia, defeated them two years later at the Battle of New Orleans. When Pancho Villa crossed our southern border in 1916, his force was engaged by troopers of the United States Cavalry. When a sabotage team landed near Long Island during World War II, an alert Coast Guardsman called in the FBI. When the threat to our infrastructures was manned bombers and intercontinental ballistic missiles, the Air Force operated radars along the Distant Early Warning Line, the Army and Army National Guard manned Nike air defense missile sites, and the Air Force and Air National Guard stayed on alert at bases across North America.

If an invader is a naval armada, an amphibious force, a fleet of bombers, or a ballistic missile, it is a military problem. Spies or saboteurs who enter the country in disguise, hide among the populace, and act on behalf of foreign governments are a counterintelligence problem.

But "cyber invaders" are not machines or people; they are packets of information. Until the electronic packets comprising a cyber invasion can be assembled and the information they contain analyzed, it is impossible to determine if the attacker is a foreign power, a criminal element, or even a US person.

Who then, should have responsibility for protecting our critical infrastructures from deliberate attack? The individual businesses that comprise the critical infrastructures are for the most part privately owned and operated. When the threat to our infrastructures was armed invasion, we did not expect owners and operators to field their own armies. When the threat was manned bombers and ICBMs, we did not expect owners and operators to acquire their own surface-to-air missile systems. Today the threat is not so well defined. In the absence of a clearly defined actor with unambiguously hostile, intent and capabilities we can see and count and compare to our own, we have to assess vulnerabilities and consider the capabilities that exist to exploit them. The basic attack tools – computer, modem, telephone connection, and software – are common across the spectrum from the recreational hacker to the information warrior. The Commission concluded that owners and operators have a responsibility to understand and take prudent steps to reduce or eliminate their own vulnerabilities – to protect themselves against the tools a threat could employ.

Government clearly has a role to play in support of owners and operators. Government alone can enunciate a policy designed to deter cyber attacks. Government alone has the authority and means to

collect information about the activities and efforts of criminals, terrorists, rogue states, and enemy nations. Government alone has the ability to bring together the resources of the nation to develop the technological tools we need to defend ourselves against the emerging threats of the 21st Century.

But who in government should take the lead? Presidential Decision Directive 39 assigns certain responsibilities to the Department of Justice and the FBI. Given the lack of knowledge available at the initiation of an attack, it is clear that any required federal response will have to be led by the Attorney General as the nation's chief law enforcement officer. Elements of a federal response may require support of the Department of Defense and other departments and agencies of government. If investigation by law enforcement discloses that a series of critical infrastructure disruptions *are* the result of deliberate attacks by a hostile nation-state, then presumably at some point the federal lead would transfer to the Department of Defense.

Asymmetric Challenges

In the current global environment, the United States has no military peer. Those seeking to oppose our interests face formidable odds on traditional battlefields, where our technology and reach cannot be challenged without significant resource investments. However, US military predominance is also the catalyst for asymmetric threats to our interests. Those who seek strategic advantage over the US may use unconventional approaches to circumvent or undermine our strengths while exploiting our vulnerabilities, placing at risk those things which we take for granted. information warfare increases asymmetric risk. Open source access to vital information by our adversaries can highlight potential vulnerabilities, and attackers using readily available tools and techniques can hide behind a veil of anonymity.

Cyber Geography

Crossing a national border with hostile intent is a recognized hostile act. Territorial waters are generally well defined, and air sovereignty is an accepted international principle. The cyber world offers new challenges. There are no borders in cyberspace. A hostile intrusion may accomplish its objectives within seconds. What constitutes an "act of war" is unclear.

Current Domestic Roles and Missions

Historically, our military forces have taken on domestic missions no other arm of government was equipped or able to perform. Examples include protecting our frontiers as the nation moved westward, surveying the nation, taming our rivers, and providing humanitarian and other support during natural disasters. Today, some domestic missions are entrusted to the National Guard, often under state authorities, and the Army Corps of Engineers. However, we have a long history, predating the Constitution, of avoiding military involvement in civilian affairs. The military's role in domestic affairs has been carefully delineated by the Constitution, Title 10, of the US Code,[8] and, most notably, by the Posse Comitatus Act of 1878.[9] Various Defense Department directives, including Military Support to Civilian Authorities[10], Military Assistance for Civil Disturbances[11], and the Department of Defense Key Asset Protection Program[12] spell out in careful detail the circumstances and extent to which military forces can be used for domestic purposes. The context of these statutes, directives and other related authorities, stays within the dimension of traditional physical security risks against military or quasi-military threats, or to protect against civil disorder.

Over the past decade, since passage of the Goldwater-Nichols Act of 1986, the Department of Defense has evolved toward increasingly effective unified military operations, drawing together the specific roles and functions of the military departments and the services under the combatant command authority of a unified commander-in-chief (CINC) whose mission may be geographic or functional in nature. Post Cold War military operations have focused primarily toward supporting national objectives in overseas theaters of operation. Under the Unified Command Plan, the Commander-in-Chief, US Atlantic Command (USCINCACOM) has responsibility for planning for land defense of the continental United States (CONUS), security operations to assist government agencies, and execution of actions on order. The Commander-in-Chief, US Space Command (USCINCSPACE) has no surface-based geographic area of responsibility, but has functional responsibilities for supporting the North American Aerospace Defense Command (NORAD) by providing the missile warning and space surveillance necessary to fulfill the US commitment to the NORAD Agreement: planning for and developing requirements for strategic ballistic missile defense and space-based tactical ballistic missile defense; and providing integrated tactical warning and attack assessment of space, missile, and air attacks on CONUS and Alaska if NORAD is unable to accomplish the assessment mission. No CINC has functional responsibility for defending the US against information warfare attacks. Command arrangements for any Department of Defense response to information warfare attacks on our domestic critical infrastructures would have to be ad hoc, or responsibility would fall by default on the Chairman of the Joint Chiefs of Staff and the Joint Staff, possibly contravening restrictions against conferring command responsibility on the Chairman[13] and the prohibition against the Joint Staff's having executive authority or functioning as an Armed Forces General Staff.[14]

Policies pertaining to domestic use of military forces in a physical security context have been evolving for two centuries. We are more than two decades into the Information Age and the cyber security issues

that come with it. Cyber issues, including interdependencies and complexities, may lead to a striking evolution in traditional defense roles -- and there will be more changes in this environment as the cyber dimension builds and evolves over future decades. Implementation and management of infrastructure protection initiatives domestically will require extensive coordination between key government agencies as well as increased coordination with state and local authorities. They will also require more direct contact between whomever is responsible for information warfare defense and the owners and operators of critical infrastructures.

A New Defense Mission?

Many in-depth explorations of information issues have already occurred, including two Defense Science Board summer studies focusing on information warfare[15] and a range of information and infrastructure-focused games to explore both offensive and defensive implications.[16] These efforts have explored policy issues and heightened awareness of information and infrastructure issues as they pertain to military operations and national security. More detailed exploration of infrastructure implications continues through the work of the Department of Defense's Critical Infrastructure Protection Working Group. However, these efforts have not yet gelled into recognition of critical infrastructure protection as a military mission. In an age of declining budgets and with force levels stretched thin across the globe, few are eager to take on a new mission that could divert resources from other, more traditional pursuits.

The Defense Department role in "providing for the common defense" against cyber threats may be in keeping with the military's traditional role of taking on missions no other arm of government is capable of performing. Applying military resources and capabilities to this emerging domestic need requires open-minded consideration of the rationale for applying military core competencies in unique ways to serve the nation. If the requirements are justified, a new or modified domestic mission may indeed be appropriate. Employing military capabilities in support of national objectives around the world will clearly remain the prime mission of the Department of Defense; however, the allocation of defense assets may need to be adjusted to support domestic infrastructure assurance missions.

Core Competencies of the Defense Department

There are specific functions that the Department of Defense can perform better than any other section of government, including some which *only* the DoD is authorized or otherwise able to perform. Defense understands emerging infrastructure risk and assurance issues better than most government and non-

government agencies and organizations. It has much to offer to support the development and integration of emerging threat and risk issues into broader national assurance and protection planning efforts. The Department of Defense's many centers of excellence and specific core competencies can contribute significantly to enhanced protection and assurance of critical infrastructures. These centers of excellence, besides supporting the Department of Defense, can also support other key government agencies and departments, at federal, state and municipal levels, and private sector assurance initiatives. Some representative Defense Department core competencies include:

Defense Planning and Training Processes

The Department of Defense routinely explores and plans for a broad range of military contingency and crisis options to allow the fullest preparation for potential global events. These planning and training processes and ways of thinking can be applied against domestic planning initiatives toward prevention, mitigation, incident and consequence management, and recovery of infrastructure events.

Computer Emergency Response Teams (CERTs)

The Defense Information Systems Agency (DISA) and Service CERTs are leaders in the development and operational implementation of a variety of information security tools, such as auditing and monitoring systems to identify intrusions into unclassified information networks. The operational experience, lessons learned, and technical insights of these teams could be applied to non-defense organizations and processes, within and outside government, to enhance cyber security in support of infrastructure assurance and protection initiatives.

Research and Development

The military services, the Defense Advanced Research Projects Agency (DARPA), the Advanced Technology Office within the Office of the Secretary of Defense, and other Department of Defense commands and agencies, have a wide range of experience and expertise in research and development of new capabilities. The technical skills resident within these offices and programs constitute an unrivaled resource that can be coupled into military operational tools, planning, and thinking. They also provide an invaluable core strength that can be integrated into assurance and protection processes.

Vulnerability Assessment Tools

A wide range of focused skills can aid in assessing vulnerabilities to physical and cyber risks, including consideration of interdependencies on other infrastructures. Some of the more important Department of Defense capabilities include:

- "Red Teaming" capabilities and insights -- available within many Department of Defense components;

- DISA's ASSIST program -- evaluating intrusion success potentials and assessing protection options for Department of Defense systems;
- The Joint Project Office for Special Technology Countermeasures (JPO-STC), Dahlgren, VA -- interdependency analysis, modeling and simulation capabilities, and other skills to facilitate vulnerability and assurance initiatives;
- Defense Special Weapons Agency (DSWA) and its Springfield Research Facility (SRF) -- vulnerability assessment teams, focusing primarily on physical interdependencies; and
- The National Security Agency (NSA) -- significant cryptographic, signals analysis, and information security expertise.

Intelligence Collection and Threat Assessment Capabilities

These are classic strengths of the Department of Defense that need to be applied toward new risk management areas.

Critical Asset Assurance Program

This initiative, already underway, will advance Key Asset Protection to incorporate a broader range of infrastructure issues, including integration of both physical and cyber security, as well as consideration of interdependencies and their potential impacts on infrastructure services.

Experience from Offensive Application of Force

Many of the offensive military concepts, experiences, and specific technological skills can be applied to more thoroughly consider and assess vulnerabilities, as well as highlight necessary protection and assurance options.

Military Support of Civil Authorities

The National Guard and the Army's Director of Military Support (DOMS) have historically played important roles in support to civil authorities, especially at the state level, but also in supporting a wide range of the Federal Emergency Management Agency's (FEMA) Federal Response Plan emergency support functions. Emerging protection and assurance options may reveal new roles for the Guard, although this will bring with it new planning and education and awareness requirements.

Potential Defense Department Roles in Domestic Infrastructure Protection

The discussions that follow are general in nature and address areas where Defense Department roles can be explored and considered. The discussions address relevant processes, assessments, and potential planning elements to consider, while recognizing that they do not cover all situations. Unique cases may require other options. Key role questions that need to be thought through include: Where does the Department of Defense have a prime responsibility and role? Where should DoD not be in the lead, and instead operate in a supporting role? Where there are clear DoD roles, when are they engaged -- at what level of threat or risk should the DoD assume the lead for the federal response?

Protection of Department of Defense owned and operated assets

Clearly, this is a Department of Defense responsibility. Risk management assessments should be conducted, not just for traditional physical security concerns, but to integrate information and physical security risk considerations. They should also consider the vulnerabilities of the assets themselves; potential vulnerabilities within vital services (power, telecommunications, logistics, key personnel, et cetera) on which the facility relies; and assess relevant threats to the facility and its key services, critical links and nodes, and the potential impact if any are denied or debilitated. Where vulnerability and threat analyses reveal plausible risks, prevention, mitigation, and contingency planning processes may be appropriate. Further, exercises and "Red Teaming" efforts may be valuable additions to the risk management process to more effectively assess risk while evaluating the quality of training and awareness, as well as response processes for the facility. The objective is to manage risk commensurate with accurate threat and vulnerability determinations, while minimizing unnecessary security investments.

Protection of privately-owned critical infrastructure assets and services where the federal government relies on specific infrastructure products or services

Prime responsibility to protect private assets belongs to the owners and operators, but a vital aspect of infrastructure and information assurance is the increasing reliance on commercial services and products by the public sector. Where the Department of Defense components (or other federal, state and municipal authorities) are reliant on these facilities, localized coordination with key infrastructure owners and operators may be called for to coordinate assurance planning. This underlines the need for greater cooperation and partnership between government and the private sector. Most owners and operators of critical infrastructures are private entities, although in some cases, key infrastructure providers are from the public sector. A Department of Defense role to assist in the protection of such assets on which DoD has a critical reliance needs also to be evaluated. Where the Department of Defense and the

owners and operators have common interests in reliability, operability, and availability, it is appropriate to institute bilateral agreements and dialogues between DoD and the owners and operators.

- In cases where major defense facilities are major customers of key infrastructure providers, there is a powerful basis for bilateral discussions focusing on the customer's reliance on infrastructure services, and the expectation that such services will be provided with reasonable levels of assurance and protection. Further, there may be rationale for a key defense facility to support assurance planning and, in certain situations, assist in facility protection at times when high-level threats are predicted through indication and warning processes.
- All parties have an interest in the protection of shared vulnerabilities (in facilities or processes), and in cooperating in assessments of related risks; similarly, they have reason to limit the disclosure of such weaknesses to other parties -- for competitiveness reasons on the part of the private sector and for effective protection on the part of the Department of Defense. Shared assessments of risk and assurance options must be mutually agreed upon and supported by formal contracts and statutory arrangements.
- If government (Department of Defense or other agency) requires identification of key links or nodes and their relevant vulnerabilities, owners and operators may find open discussion of such information threatening and may not want government participation in assessments of such risk. On the other hand, if the head of a key federal facility and the head of a key infrastructure service provider get together to discuss mutual needs and interests, as a customer or as an organization that can assist in protection and assurance, there is a foundation for common dialogue, common interest, and a possible basis for mutual agreement on joint assurance and protection initiatives. A process to consider mutual vulnerabilities, threats, and assurance options may be appropriate, with a mutual need to protect that information from broader dissemination to others (including government entities) who may not have a "need to know."

Protection and assurance planning for non-Department of Defense, federally owned and operated infrastructure assets

This is a necessary role for the Department of Defense, not as a lead agency, but rather in a supporting capacity, as coordinated through bilateral or multilateral arrangements with the appropriate federal agencies or departments. In many cases, DoD may have greater insight in considering risk, such as through vulnerability assessments (to both physical and cyber risks), threat assessment and determination processes, security implementation, and in contingency/response planning. Currently, some supporting roles are already delineated for selected situations, as in Federal Response Plan emergency support functions, where specific responsibilities of lead and supporting organizations are considered and pre-planned.

Protection and assurance planning for state and local government owned and operated infrastructure assets

The Department of Defense should engage in a supporting role, unless determined otherwise by a declared emergency. In most cases, responsibility and authority may be delegated to the National Guard, working in conjunction with law enforcement, and delineated in terms of scope and authorities through statutes and formal directives.

Role of the National Guard under federal or state jurisdiction

Where there has been a clear requirement in the past for use of Defense Department assets to support natural disaster responses, or in civil disturbances or other emergencies that required calling out the National Guard, authorities and processes are delineated in law and directives. Should the role of the Defense Department in the protection of domestic assets increase in the future, there may be additional need to engage the National Guard. This will require further delineation of authorities, as well as development of supporting resource allocation, training and exercise needs.

Protection of non-government infrastructure facilities and assets where the Department of Defense (or government) has no reliance on specific products or services.

On the surface, it may appear that the responsibility belongs solely to the owners and operators. Yet, this is an area where Defense retains some roles in providing for the common defense, to protect our population and its assets.

Recommendations

Roles and Missions

Review existing roles and missions to consider modifications based on the cyber dimension, including consideration of increased interdependencies among infrastructures and reliance on commercial products and services. Insights toward potential roles and missions should include lessons learned from recent exercises, such as Eligible Receiver and Evident Surprise, and "first-responder" assessments as a result of recent Nunn-Lugar-Domenici II legislation. To further explore such issues, the Department of Defense should consider selected domestically-focused contingencies, similar to current overseas, theater-focused Major Regional Contingencies (MRCs). In cases where there appears to be a legitimate need for an increased role by the Defense Department, it will be important to assess the threshold of risk or vulnerability where DoD should begin providing support services to non-DoD government and private sector organizations, including how to integrate DoD core competencies into other agency or organizational processes. Where potential roles for Defense are indicated, review relevant statutes, authorities, directives, training, and operational initiatives which may require modification or additions. New roles will require corresponding resource commitments.

Information Sharing, Tactical and Strategic Warning

Explore increased coordination and information sharing processes to enhance trust and sharing with non-Deparment of Defense intelligence community assets, the law enforcement community, and private sector entities. The objective of such processes is to advance strategic and tactical indications and warning, improve prevention and mitigation opportunities, and protect sensitive and proprietary insights and processes. Evaluate potential changes in information collection priorities, integration processes, and underlying authorities.

Risk Management Processes

Accelerate risk management processes within the Defense Department by integrating tools and processes for vulnerability assessments, risk assessments, and related cost-benefit considerations. From this, determine the appropriate priority of assurance and protection missions, including resource investments to enhance assurance. Classification guidelines for infrastructure vulnerability issues may require review to appropriately protect related threat, vulnerability, and other risk information.

Core Competencies

Identify the Department of Defense core competencies and highlight processes to support other national security objectives in coordination with other government agencies and departments and with the private sector. Assess how these competencies can be applied to advance prevention, mitigation, response and restoration processes pertaining to infrastructure assurance and protection.

Defense Organizational Structure

Evaluate the Department of Defense organizational structure for responsibilities pertaining to infrastructure assurance and protection. The position of such responsibilities should parallel the way these issues are considered within the White House. If the individual assigned responsibility nationally is a Special Assistant to the President or Deputy Assistant, then the level within the Department of Defense should be determined accordingly. Currently, infrastructure responsibilities are centered in an office five levels below the Secretary. Focal points for infrastructure considerations should be established within the offices of the Under Secretary of Defense for Policy, the Under Secretary of Defense for Acquisition and Technology, the Assistant Secretary of Defense for C3I, the Joint Staff, and within the Services. The Chairman of the Joint Chiefs of Staff should review the need to assign responsibility – either geographic or functional -- for information warfare defense of the continental US and make an appropriate recommendation through the Secretary of Defense to the President. Priorities and resources throughout the Department should be reviewed to fully consider and integrate infrastructure protection and assurance requirements. Where statutory changes are required, they should be proposed and implemented. These issues need to be reviewed and debated within senior Defense Department circles, with leaders of other key agencies and departments, and with our allies and trading partners, to highlight the global implications.

New Definitions

Consider new definitions in light of the emergence of information warfare and related infrastructure protection issues. Specific aspects requiring definition include: What is an act of war in the cyber dimension? Might cyber issues require changes to the War Powers Act? What does the United States consider a "cyber act of war" or "cyber hostilities"? Do our allies and key trading partners concur? Is it possible to establish and enforce borders in cyberspace? The answers may point to a need for new statutes, cooperative agreements and understandings over jurisdiction, related enforcement issues, and international law.

Critical Asset Assurance Program

Accelerate the transition of the existing Key Asset Protection Program toward a Critical Asset Assurance Program (CAAP), with improved coordination not only among Department of Defense assets and components, but also between DoD and other key federal agencies, state and local authorities, and infrastructure owners and operators. CAAP program implementation will be shaped by the results of risk management and vulnerability assessment processes for key facilities and systems, as well as by the results of bilateral discussions and mutual arrangements between lead officials of Department of Defense components and facilities, owners and operators, municipal officials, and other government leaders with whom assurance coordination agreements must be forged.

Department of Defense Critical Infrastructure Protection Working Group

Continue and strengthen the Department of Defense Critical Infrastructure Protection Working Group process, including integrating the insights from potential assurance and protection missions into the full scope of warfighting roles for the DoD.

Education and Awareness

While efforts to raise awareness of information warfare and related cyber issues are already underway throughout the Department, these efforts require additional emphasis. Training initiatives must go

beyond “information warfare” to include consideration of interconnectedness issues, reliance of one infrastructure upon another, and the resultant new risks. These initiatives need to stress the new risk environment at not only the worker level, but for senior defense leadership,

military and civilian. The increasing drive toward privatization and outsourcing -- use of commercial products and services -- represents a particularly significant change in the way the Department of Defense does business, inserting new "denial of service" potentials that have not been mainstream considerations of DoD in the past. These issues highlight the need for integration of physical and cyber security processes and protections , as well as the need to implement effective use of encryption and other best practices to protect not just classified material, but sensitive, unclassified information.

Conclusions

The changing risk environment, with emerging cyber vulnerabilities and threats, requires an exploration of potential Department of Defense roles in protecting and assuring critical domestic infrastructures, especially in light of their increasingly interconnected and complex nature. There have been fundamental changes; such as DoD's use of commercial off-the-shelf (COTS) systems and reliance on private sector owned and operated infrastructures. The trend is toward even more interdependent processes. The very culture of how we conduct business and interrelate is being transformed.

The means by which we protect our national security and economic prosperity requires review, including consideration of future roles for the Department of Defense in "providing for the common defense" of our nation within our borders. Society may not be ready to accept an increased role by DoD in assisting in the protection and assurance of critical infrastructures – and Defense itself may not be ready to take on such roles. Yet it is time for DoD to begin exploring the implications of an increasingly interconnected and interdependent society. It is time to consider domestic military roles in the context of providing essential services for domestic infrastructure emergencies, and integrating and leveraging the core competencies of Defense in such a way that the freedoms of society are not perceived as being at risk. Increased interagency coordination, especially with the Department of Justice and law enforcement, and public/private sector coordination in a spirit of trust and mutual assurance are necessary.

Achieving the appropriate balance will not be easy, however, it appears necessary based on emerging societal needs and on federal responsibilities for national security and economic prosperity. The sky is not falling -- investments cannot and should not be made to protect everything. But now is the time for thoughtful consideration, assessment, education, and debate. Some efforts may require immediate attention based on risk assessments of plausible threats and vulnerabilities, integrating physical and cyber dimensions and the increased interdependencies, complexities, and reliances among infrastructures. Missions must be adopted with care and implemented gradually to balance the needs for national security, societal rights, and economic prosperity. And the time to act is now.

---

[1] A National Security Strategy for a New Century, the White House, May 1997, page i.

[2] Carl von Clausewitz, On War, edited and translated by Michael Howard and Peter Paret, Princeton University Press, 1984, pages 595-96.

[3] Major General John K. Herr and Edward S. Wallace, The Story of US Cavalry, 1775-1942, Boston, Little, Brown and Company, 1953, pages 231-237.

[4] Ronald H. Bailey and the Editors of Time-Life Books, The Home Front: USA., Time-Life Books, Alexandria, Virginia, 1977, pages 115-116; Francis Russell and the Editors of Time-Life Books, The Secret War, Time-Life Books, Chicago, 1981, pages 52-55.

[5] "US Defense Policies Since World War II," AUSA Background Brief No. 70, Association of the US Army, March 1996.

[6] A National Security Strategy for a New Century, the White House, May 1997, page 8.

[7] Ibid., page 9.

[8] Title 10, sections 3062 and 8062 cite, "It is the intent of Congress to provide an [Army/Air Force] that is capable, in conjunction with the other armed forces, of (1) preserving the peace and security, and providing for the defense, of the United States, the Territories, Commonwealths, and possessions, and any areas occupied by the United States; (2) supporting the national policies; (3) implementing the national objectives; and (4) overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States."

[9] 18 USC 1385: *Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.*

[10] DoD Directive 3025.1, "Military Support to Civil Authorities (MSCA)," January 15, 1993

[11] DoD Directive 3025.12, "Military Assistance for Civil Disturbances," February 4, 1994

[12] DoD Key Asset Protection Program (KAPP)," June 26, 1989

[13] 10 USC 163(b)(1)

[14] 10 USC 155(e)

[15] The Defense Science Board Task Force on Investments for 21st Century Military Superiority (1995) and the Defense Science Board Task Force on Information Warfare (Defense) (Nov 1996)

[16] There have been a broad series of games. Some of the more well-known: (a) Rand's "The Day After …." Game series (1995), sponsored by ASD/C3I, focusing on strategic information warfare, (b) Evident Surprise, a series of information war games sponsored by US Atlantic Command in 1996 and 1997, (c) Rand's "The Day After ….in the Strategic Infrastructure" Game series (1996), sponsored by ASD/C3I and OUSD (Policy), focusing on strategic infrastructure issues, and (d) Eligible Receiver, sponsored by the Joint Staff in 1997.