Cybersecurity Connection

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 13
Cybersecurity Connection

Rick White, Ph.D.
University of Colorado, Colorado Springs

1

Cybersecurity Connection

As previously mentioned, in July 1996 President Clinton appointed a Commission on Critical Infrastructure Protection in response to the 1995 Tokyo Subway Attacks and Oklahoma City bombings.

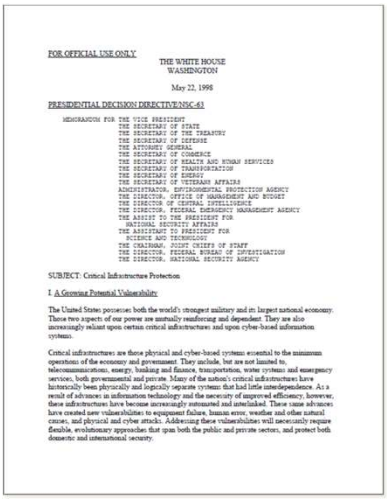
2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

As was pointed out, the Commission's report in October 1997 prompted President Clinton to issue **PDD-63** in May 1998 creating the framework for today's critical infrastructure protection program, currently managed by the DHS Office of Infrastructure Protection.



FOR OFFICIAL USE ONLY

THE WHITE HOUSE
WASHINGTON

May 22, 1998

PRESIDENTIAL DECISION DIRECTIVE/NSC-63

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF VETERANS AFFAIRS
ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
THE ASSIST TO THE PRESIDENT FOR
NATIONAL SECURITY AFFAIRS
THE ASSISTANT TO PRESIDENT FOR
SCIENCE AND TECHNOLOGY
THE CHAIRMAN, JOINT CHIEFS OF STAFF
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: Critical Infrastructure Protection

I. A Growing Potential Vulnerability:

The United States possesses both the world's strongest military and its largest national economy. These two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attack. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

3

Esc

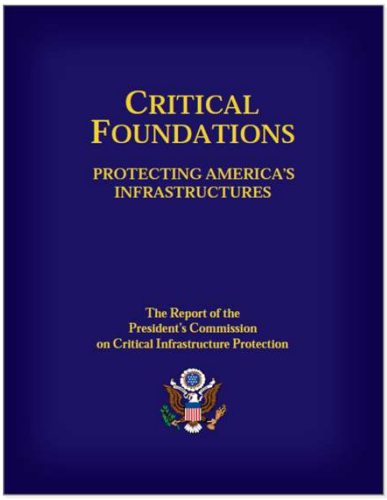
3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

What was not mentioned previously was the findings from the report...



4

Esc

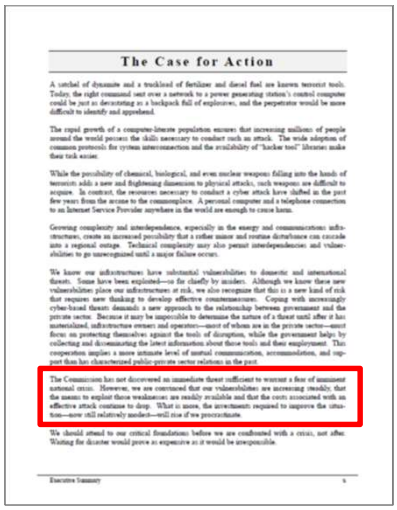
4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

The 1997 Commission report found **no immediate threat** to the nation's infrastructure...


The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the access to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructure, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about these tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit these weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investment required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

Executive Summary

5

Esc

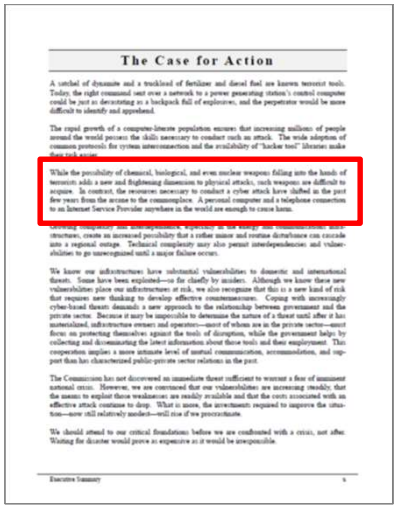
5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

However, the report was the first to raise a concern about cybersecurity.


The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the access to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructure, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about these tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit these weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investment required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

Executive Summary

6

Esc

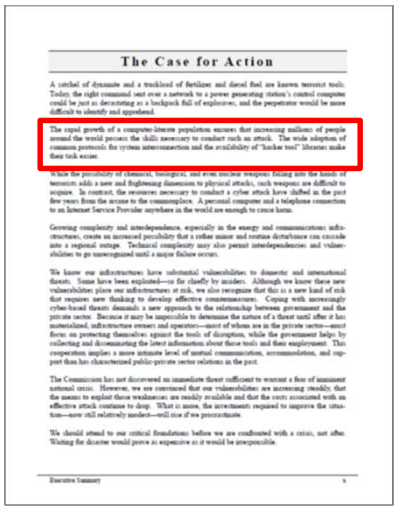
6

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

According to the Commission, the rapid assimilation of computer networks into infrastructure operations **employed the same computer hardware and protocols that were facilitating the explosive growth of the Internet.**


The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the means to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructure, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about these tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investment required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

Executive Summary

7

Esc

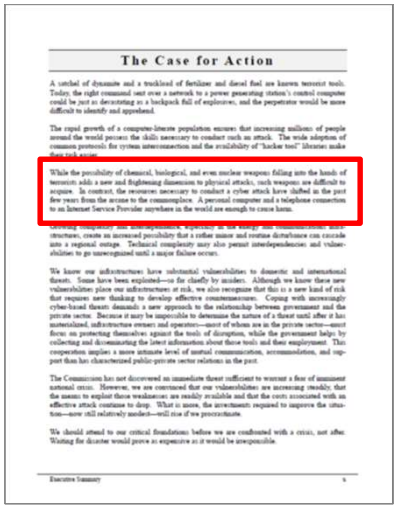
7

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

Once isolated systems were now accessible online to a growing pool of hackers with the knowledge and skills to do harm.


The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the means to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructure, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about these tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investment required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

Executive Summary

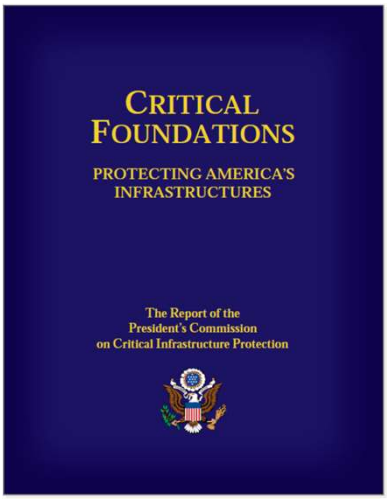
8

Esc

8

Cybersecurity Connection

The report concluded that the threat and vulnerability of cyber attack against the nation's infrastructure was both real and growing.

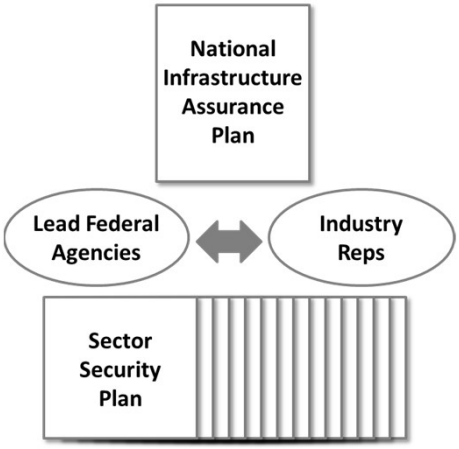


9

Cybersecurity Connection

PDD-63 Framework

- A **Lead Federal Agency** was assigned responsibility for each sector.
- Their job was to **work with industry representatives** to develop corresponding **Sector Security Plans.**
- The individual Sector Security Plans were to be integrated into an overarching **National Infrastructure Assurance Plan.**



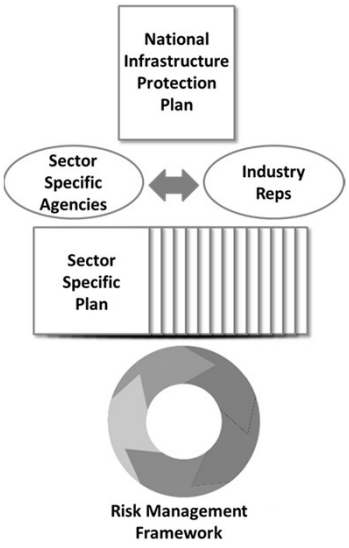
10

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

- HSPD-7 issued by President Bush in December 2003 made some modifications, but kept the PDD-63 framework intact.
- But because 9/11 had been a physical attack, the focus was primarily on physical protection of critical infrastructure.



11
Esc

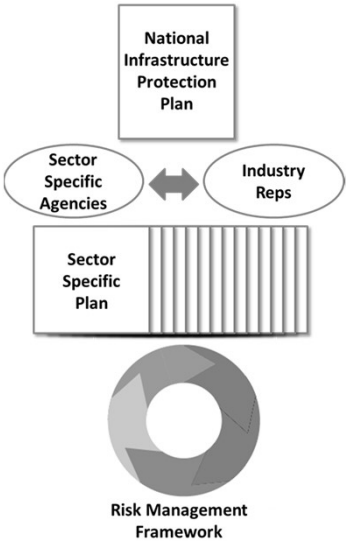
11

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

- PPD-21 issued by President Obama in February 2013 also retained the PDD-63 framework.
- **But due to a series of high-profile cyber attacks, PPD-21 returned emphasis to cybersecurity.**



12
Esc

12

Cybersecurity Connection

- The worst disaster in US history, outside the Civil War, was the 1900 Galveston Hurricane.
- It killed upwards to 6,000 people.
- **A coordinated cyber attack against critical infrastructure could be worse.**

13

Cybersecurity Connection

Top 3 Concerns

1. Simultaneous meltdown of two nuclear power plants.
2. Shutdown the entire North American electric grid.
3. Undermine the Federal Reserve system.

14

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

Remember

Homeland security is about safeguarding the US from domestic catastrophic destruction.

15

Esc

15

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Connection

Domestic Catastrophic Destruction

Two manmade means for catastrophic destruction: 1) WMD, and 2) subverting critical infrastructure.

16

Esc

16

Cybersecurity Connection

HS/CS Connection

Cybersecurity is essential to critical infrastructure protection which is essential to homeland security.

17

Esc

17

Conclusion

Questions?

18

Esc

18