Cyberspace Security & Safety

Richard O. Hundley, Robert H. Anderson,
Anthony C. Hearn, Willis H. Ware

DRU-530-ARPA
October 1993
Prepared for Advanced Research Projects Agency

This Draft is intended to transmit preliminary results of RAND research. It is unreviewed and unedited. Views or conclusions expressed herein are tentative and do not necessarily represent the policies or opinions of the sponsor. Do not quote or cite this Draft without permission of the author.
PREFACE

This paper discusses a new and emerging national problem area, the security and safety of U.S. information systems operating in cyberspace, and proposes a new national program to deal with this problem.

The work reported on here is an outgrowth of three recent RAND activities:

(1) Research conducted during 1989-1992 for the Assistant Secretary of Defense (C3I) on the technological changes confronting military intelligence over the next 10 to 20 years, including the many ramifications of information technology.

(2) A RAND-sponsored workshop on "The Effects of the Information Revolution on Society." This workshop explored the many changes that the information revolution is likely to bring about in society.

(3) A workshop on "Future Technology-Driven Revolutions in Military Operations" which RAND conducted for the Advanced Research Projects Agency (ARPA) in 1992. This workshop explored the potential for hostile actions in the "information realm" as a future tool of warfare.

The insights gained in these three studies led directly to this effort.

This research was sponsored by the Director of ARPA, under the Applied Science and Technology Program of RAND's National Defense Research Institute (NDRI). NDRI is a federally funded research and development center sponsored by the Office of the Secretary of Defense and the Joint Staff.
Cyberspace Security & Safety (CSS)

An Emerging National Problem Area

October 1993

This paper discusses a new and emerging national problem area, the security and safety of U.S. information systems operating in cyberspace, and proposes a new national program to deal with this problem.
We begin the paper with a short discussion of "cyberspace": what it is, what is going on there, and why it is important. Next, we outline the emerging potentials for:

- Evil, criminal or hostile actions in cyberspace.
- "Bad actors" in cyberspace, carrying out these "evil" actions.
- Threats to U.S. interests, as a result of the bad actors carrying out hostile actions in cyberspace.

Following that, we discuss what needs to be done to cope with this problem: specifically, a national program in Cyberspace Security and Safety (CSS). We conclude with an outline of the elements of such a national program.
“CyberSpace”: What’s Going On There?
(1 of 2)

- Regarding Information
  - "All" information going digital & electronic
  - Often supplanting all paper records

- Regarding Transactions
  - Explosive growth in electronic data interchange & electronic commerce
  - For commercial, financial & governmental transactions
  - Both nationally & internationally
  - With the "value-added" increasingly information-based

- Regarding Physical Infrastructures
  - Physical infrastructures increasingly controlled by information systems
  - Power grids, air traffic control, telecommunications, etc.

- Regarding Connectivity
  - Increasing worldwide, universal interconnectivity
  - With exponentially increasing bandwidth
  - With increasing porosity of national borders
  - With millions of new entry points every year & few security safeguards

As one consequence of the electronic digitization of information and the worldwide internetting of computer systems, more and more activities in the U.S. and throughout the world are mediated and controlled by information systems. This includes human activities of all kinds:

- Activities involving the production, manipulation, storage and dissemination of information.
  - Including research and educational activities, engineering and industrial processes, etc.
  - With more and more information going digital and electronic, often supplanting all paper records.

- Activities involving all manner of transactions:
  - Commercial business and financial transactions (with the “value-added” in these transactions increasingly information based).
  - Operations of civil governments at all levels (national, regional, and local).
  - Political activities.
  - Both public and private social interactions.

- Activities involving the operation and control of essential physical infrastructures -- power grids, air traffic control, telecommunications, etc.
At the same time, there is increasing worldwide *interconnectivity*, with exponentially increasing bandwidth, increasing porosity of national borders, millions of new entry points every year, and few security safeguards.

This global world of internetted computers and communications systems in which more and more of these human activities are being carried out has come to be called "cyberspace."
As time goes on, these internetted information systems operating in cyberspace form increasingly large-scale, complex systems, in which small disruptions can have amplified effects, creating unknown instabilities and vulnerabilities.

At the same time, the U.S. is becoming increasingly dependent on foreign information hardware and software. The same is also true for all other nations. Today there is little or no examination of this foreign hardware by anybody -- in the U.S. or any other nation -- for hidden anomalies.

All of these activities in cyberspace are becoming more and more transnational, beyond the effective control of the U.S. or any other national authorities.

Finally, more and more DoD capabilities are becoming increasingly dependent on commercial information systems which are immersed in this cyberspace environment.
The information systems mediating and controlling these various activities in cyberspace are subject to a broad spectrum of "evil actions," as illustrated in this chart. These include attacks on the data contained within the systems, the programs and processing hardware running those systems, and the environment (communications, networks, etc.) in which they operate. The spectrum of possible evil actions includes:

- Inserting false data or harmful programs (viruses, worms, etc.) into information systems.
- Stealing valuable data or programs from a system, or even taking over control of the operation of a system.
- Manipulating the performance of a system, by changing data or programs, introducing communications delays, etc.
- Disrupting the performance of a system, by causing erratic behavior or destroying data or programs, or by denying access to the system.

All of these evil actions can be done surreptitiously. Many of them can be done remotely, at a great distance from the target system -- sometimes from the other side of the world -- via a series of internetted, intermediary systems. Taken together, the surreptitious and remote nature of these actions can make their detection difficult, and the identification of the perpetrator even more difficult.
Potential “Bad Actors” In This World: Another Wide Spectrum

- Criminals
  - For personal financial gain, revenge, etc.
- Hackers, Zealots, Madmen, or Disgruntled Employees
  - To satisfy personal agendas
- Terrorists or Insurgents
  - To advance their cause
- Commercial Organizations
  - For industrial espionage or to disrupt competitors
- Nations
  - For espionage or economic advantage or as a tool of warfare

This gives rise to a new set of vulnerabilities -- for governments, the military, businesses, individuals, and society as a whole -- that can be exploited by a wide spectrum of “bad actors” for a variety of motives, as indicated on this chart.

In this cyberspace world, the distinction between “crime” and “warfare” is blurred. The resources required for a nation to mount a computer-based attack on the military, economy, or society of another nation (presumably an act of war) are not necessarily any larger than those required for an individual to mount a computer-based criminal attack on another individual, company, bank, etc. In each case all that may be required are one (or at most a few) smart computer experts with computer terminals hooked into the worldwide network.

This blurring of the distinction between “crime” and “warfare” in cyberspace also blurs the distinction between police responsibilities, to protect U.S. interests from criminal acts in cyberspace, and military responsibilities, to protect U.S. interests from acts of war in cyberspace.
Potential Threats To U.S. Interests

In Civilian Society & Economy
- Violations of individual or organizational privacy
  - For various motives, including blackmail
- Theft of valuable intellectual property
- Misappropriation or disruption of financial transactions
- Disruption of commercial & industrial activities
- Disruption of critical infrastructures
  - Power, communications, transportation

In the Military Arena
- Disruption of C3I systems
- Disruption of weapon & platform control systems
- Disruption of logistics
- Theft of classified information

These possibilities for evil actions in cyberspace, and this spectrum of potential bad actors, lead to a new set of potential threats to U.S. interests, in both the civilian society and economy, and in the military arena. This chart indicates some, but by no means all, of these new and emerging threats to U.S. interests. (A number of more specific illustrations of these threats are given in the Appendix.) We have already seen examples of several of these actually occur.\(^1\)

Protecting government, business, individuals, and society as a whole against these evil actions by bad actors in cyberspace we call "cyberspace security."

---

\(^1\) Two (among many) notable examples were the "Internet Worm," which disrupted activities on the Internet in 1988, and the "Hannover Hacker," who stole information from computer files all over the world during 1986-1988 and sold it to the KGB. (The story of the Hannover Hacker is told in *The Cuckoo's Egg* by Clifford Stoll.)
Safety Hazards In Cyberspace

- Unintended dangerous situations, caused by unanticipated events -- such as:
  - Disruption by software errors, e.g.
    - Telephone outages
    - "Fly-by-wire" airplane failures
    - Control system breakdowns
  - Disruption by hardware errors, e.g.
    - Component failure
    - Cable severance
    - Natural disasters (flood, lightning, etc.)
- Protection against these hazards requires a program of cyberspace "safety", including:
  - Fault tolerant software, hardware & system architectures
  - Backup systems for natural disasters

In addition to deliberate threats, information systems operating in cyberspace, when embedded in their operational environments, can also cause unforeseen actions or events -- without the intervention of any bad actors -- that create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded.

Such safety hazards can result from both software and hardware errors. These can range from something as simple as a farmer accidentally cutting a fiber-optic cable while burying a dead cow (which closed four of the FAA’s 20 major air-traffic control centers for over five hours in May 1991) to the software error that caused a major breakdown in AT&T long distance service in 1992.

With the expected increased reliance on information systems for many of the day-to-day transactions and activities in our society, we expect this problem to increase in the future. Protection against this additional set of cyberspace hazards we call "cyberspace safety."

In the new cyberspace world, government, business, individuals, and society as a whole require both "security" and "safety" protections: i.e., a comprehensive program of cyberspace security and safety (CSS).
### Whose Problem Is It?
#### Everybody’s & Nobody’s

<table>
<thead>
<tr>
<th>U.S. Federal Government</th>
<th>U.S. State &amp; Local Governments</th>
<th>Non-Governmental Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Intelligence Agencies</td>
<td>- Law Enforcement Agencies</td>
<td>- Business &amp; Professional Associations</td>
</tr>
<tr>
<td>- Defense Department</td>
<td>- Regulatory Agencies</td>
<td>- Vendor Organizations</td>
</tr>
<tr>
<td>- Federal Law Enforcement Agencies</td>
<td></td>
<td>- Industry Standard-Setting Bodies</td>
</tr>
<tr>
<td>- Civilian Regulatory Agencies</td>
<td></td>
<td>- Private Businesses</td>
</tr>
<tr>
<td>- Other Civilian Agencies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Governments of Other Nations</th>
<th>International Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Intelligence Agencies</td>
<td>- United Nations</td>
</tr>
<tr>
<td>- Ministries of Defense</td>
<td>- Supra-National Governing Bodies</td>
</tr>
<tr>
<td>- Law Enforcement Agencies</td>
<td>- Interpol</td>
</tr>
<tr>
<td>- Other Agencies</td>
<td>- International Standards Bodies</td>
</tr>
</tbody>
</table>

Responding to this new, emerging security and safety “threat” and providing these CSS protections requires activities coordinated across many organizational boundaries: military and civilian agencies of the U.S. government; federal, state and local agencies; both governmental and non-governmental entities; the U.S. and other nations; and national and international organizations. Today this is “everybody’s” problem, and therefore “nobody’s” problem. It falls into all of the “cracks.”
Another Aspect of the Problem

- Information technology will not sit still
  - While we solve this problem

- It will continue to evolve at an exponential rate

- Any “solution” to this problem must keep up with
  - Advances in information technology
  - New applications of information technology

- This will be a major challenge

There is another aspect to the problem, which makes it even more difficult: information technology is not static. Rather, it is evolving at an ever increasing rate, with new technological capabilities and new applications -- throughout all corners of society -- arising all the time. Information technology has been doing this for some time now, and it will continue to do this for the foreseeable future.

This makes the “solution” to the CSS problem even more difficult. Any solution must not only solve today’s problem, but also tomorrow’s. It must keep up with future advances in information technology, and new applications of that technology arising in the future.

This will be a major challenge. Indeed, past U.S. efforts at “computer security” have largely failed this challenge.2 Somehow, we will have to do better this time.

---

2 The U.S. has had a program in computer security since the 1960s. In spite of all of these efforts, however, the U.S. is full of insecure computers today. There are several reasons for this (c.f. the discussion on the next page), but one primary one is that computer technology and its applications have progressed and evolved faster than computer security efforts could keep up.
What has been done in the past? As we have just said, the U.S. has had a program in computer security since the 1960s. The driving force in this program has been the U.S. defense establishment. The focus of the program has been:

- On threats of the type perceived by the defense establishment
  - Specifically, penetration activities of foreign intelligence agencies
- On protection of the secrecy of information contained in computer systems
  - Not on protection of the integrity of that information, or protection against denial of service
- On governmental and industrial participants in the defense establishment
- Largely on operating systems for stand-alone systems
  - Which was the original problem addressed in the 1960s

As a result of this focus, as well as the continual evolution of information technology mentioned previously, the protective techniques and safeguards developed during this 30 year period of computer security efforts have been largely ignored: ignored not only by the civilian world, to which they were not primarily directed, but also in large part by the defense world as well.
In effect, these existing computer security techniques and safeguards have been deemed either:

*Irrelevant*

- Not addressing the real information system security problems faced by a given organization or individual.

or

*Ineffective*

- Not providing an adequate solution to those problems.

or

*Uneconomic*

- Costing more (in money or time or user inconvenience) than they were worth.

by their intended users, or sometimes all three.\(^3\)

Recently, with the passage of the Computer Security Act of 1987, this narrow focus of U.S. computer security efforts has been broadened slightly; the National Computer Systems Laboratory (NCSL) was chartered as part of the National Institute of Standards and Technology (NIST) to establish security standards and guidelines for unclassified systems throughout the federal government. This is broader than the previous focus on the world of defense, but it still leaves most U.S. information systems and networks out.

---

3 Perceptions that these computer security safeguards are irrelevant and uneconomic are particularly prevalent in the non-defense world, both within and outside the federal government.
What needs to be done differently in the future? What lessons can be learned from the past, to be applied to the future?

It is clear today, in the post-Cold War world, that penetration by foreign intelligence agencies is not the only important threat that U.S. information systems and networks face, and that cyberspace vulnerabilities in the military arena are not the only ones with which the U.S. should be concerned. The U.S. should be equally concerned with cyberspace vulnerabilities affecting the civilian society and economy.\(^4\)

Because of this, in the future U.S. cyberspace security and safety activities should have a national focus, not just a defense focus. They should treat all societal vulnerabilities, not just those of one portion of society; they should address information integrity and service availability, as well as confidentiality; and they should have a total system and network focus, not just a focus on components (e.g., operating systems).

Future U.S. cyberspace security and safety activities should also have the active involvement of non-governmental organizations, including business and professional associations, vendor organizations, industry standard-setting bodies, and private business.\(^5\) And better ways of motivating key groups and individuals to participate must be developed.

---

\(^4\) Over the near term, “crime” in cyberspace may be a bigger problem than “war” in cyberspace.

\(^5\) The relative lack of involvement of such non-governmental organizations in past computer security efforts was another important reason for their ineffectiveness.
What is required then, is a program that addresses both:

- Security in cyberspace
  - Protection against evil actions by bad actors in cyberspace
- Safety in cyberspace
  - Reasonable assurance that information systems operating in cyberspace do not cause actions or events that create unintended dangerous situations for themselves or for the environments (including people) in which they are embedded.

This program must keep up with future advances in information technology and in the application of that technology. Also, it must be national in scope -- covering both governmental and non-governmental information systems, both military and civilian systems -- because the problem is national in scope.

In other words, a national program of cyberspace security and safety.
What Should The Purpose Of This Program Be?

The broad overall purpose of the endeavor of which the proposed ARPA program is merely the beginning should be:

- To protect U.S. interests in & relating to Cyberspace,
  Including
  - Governmental & non-governmental interests
  - Military & civilian interests
  - Economic & social interests
- While still allowing the nation to reap maximum benefits from emerging information technologies

This national CSS program should have a broad overall purpose:

- To protect all important U.S. interests in and relating to cyberspace.

These include both military and civilian interests, both governmental and non-governmental interests, and including economic and social interests.

And the program should devise ways of protecting these interests while still allowing the nation to reap maximum benefits from information technology -- both today's technology and tomorrow's technology.
To be truly effective, this program requires a broad scope, in six interrelated dimensions:

- Covering a wide range of information systems operating in cyberspace, from transaction systems, through scientific and engineering applications, to systems for real-time control.

- Covering a broad spectrum of evil actions, being perpetrated on those systems in cyberspace.

- Covering a broad spectrum of bad actors, perpetrating those evil actions, including criminals, hackers or zealots or madmen, terrorists or insurgents, commercial organizations, and other nations.

- Covering a broad spectrum of safety hazards that cyber-systems might pose for their environments, for operational personnel, for the public at large, and for other systems.

- Covering a wide range of U.S. interests, threatened by those evil actions, bad actors, and safety hazards, including military and civilian interests, and both governmental and non-governmental interests.

- Focusing on a broad user community which would ultimately apply the protective techniques and procedures developed in the program, including U.S. federal, state, and local governmental agencies, a wide variety of non-governmental entities in the U.S., governments of other nations, and international organizations.
This chart lists six program elements deemed necessary for a comprehensive and effective CSS program:

- Assessment of cyberspace vulnerabilities and hazards.
- Development of technical safeguards.
- Definition of "non-technical" protective procedures.
- Development of a family of solution strategies.
- Demonstration projects.
- Outreach and handoff.

We discuss each of these in the following charts.
Assessment of CyberSpace Vulnerabilities & Hazards

- Systematic analysis of points of exploitation, failure modes, architectural weaknesses, & safety hazards of systems & networks
  - Including those involved in commercial, financial & governmental activities
  - Including those controlling physical infrastructures
- Identification of "critical national systems and networks," in both the governmental & non-governmental realms
  - With the development of prioritized vulnerability & hazard roadmaps for these systems & networks
- The use of "red teams" focused on specific subsets of the information system / cyberspace spectrum
  - As one mechanism for carrying out this systematic analysis & developing these roadmaps
- Demonstration of selected (and dramatic) vulnerabilities & hazards, to appropriate audiences
  - To focus their attention on the problem

One of the first steps must be to develop a more detailed understanding of the dimensions of the information systems security and safety problem confronting the U.S. This effort should include:

- The systematic analysis of points of exploitation, failure modes, architectural weaknesses, and safety hazards of U.S. information systems and networks, including those involved in commercial, financial and governmental activities, as well as those controlling physical infrastructures.⁶

- The identification of "critical national systems and networks," in both the governmental and non-governmental realms, which should receive special attention in the program, and the development of prioritized vulnerability and hazard roadmaps for these systems and networks.⁷

- The demonstration of selected (and dramatic) vulnerabilities and hazards uncovered in this effort, to appropriate audiences, to focus their attention on the problem.

---

⁶ The use of "red teams" focused on specific subsets of the information system / cyberspace spectrum may be one useful mechanism -- but obviously not the only one -- for carrying out this systematic analysis.

⁷ A system or network may be deemed "critical" for many different reasons: because it provides essential support to vital physical or financial infrastructures; because its compromise could jeopardize the safety or well being of large numbers of U.S. residents, or their financial security, or even merely their piece of mind; because its pervasive use for valued functions in society offers a widespread target for bad actors; because it plays a vital national security role; etc.
Development of Technical Safeguards

- For systems and networks
- With an emphasis on network security & safety, as well as computer security & safety
  - With particular emphasis on heterogeneous networks
- Including techniques such as:
  - Dynamic real-time monitoring of cyberspace
    - For "exception reporting" on noteworthy developments & changes, and unsafe or hazardous circumstances
    - Including software "police agents" able to inhabit & explore cyberspace
  - Pattern signature & authentication tests of chips, circuits, & software
    - To serve as the technical basis for a registry of authorized hardware & software, and as a means of detecting unauthorized modifications
  - As well as techniques for individual system security
- Including testing of the safeguards that are developed

The development of technical safeguards is an obvious, integral component of the CSS program. These safeguards should emphasize network security and safety, as well as computer security and safety, with particular emphasis on heterogeneous networks. The detailed assessment of cyberspace vulnerabilities and hazards, carried out in the previous program element, will give shape and direction to these developments.

This chart lists only a few illustrative safeguarding techniques. Many more are necessary, and with focused invention, many more are likely to be available.

This effort will obviously include testing of the safeguards that are developed.

---

8 In the past, ARPA, NSA and other U.S. research organizations have done some work on computer security. However, little has been done on network security. To date, cyberspace safety has been addressed in only a few areas: primarily DoD weapon systems, fly-by-wire aircraft, medical instrumentation, and nuclear power installations.
Definition of Useful & Necessary
"Non-Technical" Protective Procedures

Candidates include
- Monitoring arrangements
  - Both national and international
  - For early warning, identification of transgressors, & post-event analysis
- Mandated system & network protective measures
  - At national & international levels
  - For "critical" systems & networks
  - With graduated levels of protection
  - Which are "affordable"
- National & international sanctions
  - Against "infractions" or unsafe systems occurring in cyberspace
- Education & training, to increase user awareness of:
  - Need for CSS measures
  - The things users can & should do

The development of technical safeguards, no matter how good they are, will not be enough to solve the CSS problem all by themselves.\textsuperscript{9} Also required are:

- Mandates (legal or otherwise), to compel or at least strongly urge people to use available protective measures on their information systems.\textsuperscript{10} The mandated measures must appear reasonable and "affordable" to their user community.

- Sanctions (legal or otherwise) against the perpetration of "evil actions" or the operation of unsafe systems in cyberspace. Because of the transnational character of many/most activities in cyberspace, these sanctions may ultimately have to be international in scope to be truly effective.

- Monitoring arrangements in cyberspace, for early warning of adverse events, identification of transgressors, and post-event analysis. Once again, because of the transnational character of cyberspace, these monitoring arrangements may ultimately have to be international in scope.

\textsuperscript{9} Over the last 30 years, computer security research in the U.S. has developed a number of such technical safeguards. Today, most of the computers operating in the U.S. do not use many, most, or even any of these safeguards.

\textsuperscript{10} There is an analogy here with the need for laws requiring the use of seatbelts in automobiles, or the wearing of helmets by motorcyclists.
Education and training activities -- extending throughout the user, vendor, and management communities in both the governmental and non-governmental realms -- to increase user and management awareness of the need for CSS measures, and of the things that users can and should do to combat these new threats.\textsuperscript{11} 

\textsuperscript{11} The lack of adequate and comprehensive education and training activities was another important reason for the ineffectiveness of previous computer security efforts.
Development of a Family of Solution Strategies

- Made up from the “menu” of technical safeguards & non-technical protective measures developed in other program elements
- Tailored to cover a range of vulnerabilities, operational environments, & criticalities
- To provide a set of solution options
  - From which individuals & organizations can select those most suited to their specific circumstances

The two previous program elements will provide a menu of technical safeguards and non-technical protective measures. These should be used as the ingredients in a family of solution strategies, tailored to cover a range of vulnerabilities, operational environments, and system criticalities.

This family will provide a set of solution options, from which individuals and organizations can select those most suited to their individual circumstances.
Demonstration Projects

- To demonstrate elements of the family of solutions

- To interested audiences & potential implementing agencies

This is a key part of the overall CSS program. As elements, and integrated combinations of elements, of the family of solutions are developed, they should be demonstrated to interested audiences and to potential implementing agencies.
Since the ultimate success of this program depends on the widespread application of CSS-developed technical safeguards and protective procedures throughout the U.S. economy and society, the CSS “lead agency” -- whoever that may be -- cannot do it all or do it alone. Other implementing organizations, in both the governmental and non-governmental realms (and perhaps even in the international realm), must adopt and apply the CSS-developed solutions. Bringing this about requires a conscious program of “outreach” as part of the overall CSS program.

To be most effective, these outreach activities should extend throughout the entire program, gradually increasing in intensity as the program proceeds, rather than just being concentrated at the end.

12 We discuss the characteristics required in a CSS “lead agency” later in this paper.
Outreach & Hand-Off
(2 of 2)

Some illustrative outreach activities

- Involvement of representatives from selected user communities in "red teams" carrying out vulnerability & hazard assessments
- Demonstration of selected vulnerabilities & hazards to various organizations
  - To stimulate their involvement in the CSS program
- Demonstration of new technical safeguards, developed during the CSS program, to similar audiences, for a similar purpose
- Involvement of other governmental agencies & non-governmental entities in the identification & definition of non-technical protective procedures. Useful agencies & organizations to involve could include:
  - Federal & state law enforcement agencies
  - Governmental regulatory agencies & non-governmental standards-setting bodies
  - Associations of information-technology producers & users
- Involvement of other agencies & organizations, both governmental & non-governmental, in the development & critique of the family of solution strategies & in the conduct of demonstration projects

This chart lists some illustrative activities that could be included in such an outreach program.

If these outreach activities -- and others like them -- are done well, they should greatly facilitate the hand-off of the CSS-developed technical safeguards and protective procedures to the ultimate users, military and civilian, governmental and non-governmental, throughout the U.S. economy and society.
This program is one of large magnitude, addressing a very large, complex set of problems. Initially, a major, multi-year program is clearly required to fulfill the stated objectives and accomplish the overall purpose. Ultimately, the duration of this initial program will be determined not only by the pace of technical progress in that program, but also by the rate at which the hand-off to the ultimate users can be carried out. Once this hand-off has been achieved and the desired degree of CSS protections attained throughout the U.S., a permanent "sustainer" program should be established, to maintain these protections over time, as information technology evolves.
As indicated earlier, the six suggested program elements are interrelated. This chart indicates one possibility for the initial program phasing. The assessment of cyberspace vulnerabilities and hazards should obviously begin first: a better understanding of these vulnerabilities and hazards is necessary as a foundation for all other program activities.

The development of technical safeguards and the definition of protective procedures come next. They can (and probably should) be done in parallel, with a great deal of back-and-forth interaction. When they begin is open to question. They certainly should begin no later than the beginning of the second year; they could begin part way through the first year.\textsuperscript{13}

The scheduling of subsequent program elements -- on the development of the family of solutions and the demonstration projects -- should depend on the pace of accomplishment in these three initial elements. The chart shows them nominally beginning sometime during the second year; that may or may not turn out to be realistic.

Finally, as indicated earlier, the outreach activities should begin early in the program and continue throughout.

\textsuperscript{13} The first year of the program could usefully be devoted to a detailed assessment of cyberspace vulnerabilities and hazards, to develop a better understanding of the problem, increase awareness of it in relevant U.S. circles, and lay a firm foundation for subsequent program elements. This would provide a very careful and deliberate start to the CSS program. However, it is not necessary to start off this slowly, if a more aggressive beginning is desired.
What Should This Program Be Called?

- The name chosen for this new program should:
  - Convey a sense of what the program is about
  - Capture people's attention & interest
  - While not raising any "bad" connotations
    - E.g., spying, invasion of privacy, attacks on information systems
- Three possibilities include:
  - **Cyberspace Security & Safety**
    - Has a newness that should capture people's attention
    - Provides most vivid image of program
  - **Security & Safety in the National Information Infrastructure**
    - Less novel
    - But invokes momentum of National Information Infrastructure
  - **Information Systems Security & Safety**
    - Most conventional & maybe "safest"
    - But may not convey adequate sense of program's scope & importance

What should this program be called? This is not merely an idle question, since the name chosen can have a lot to do with the initial public perception of the program. A "good" name can facilitate outreach. A "bad" name can cause problems. Careful thought should be given to this in setting up the program.

The name chosen for this new program should convey a sense of what the program is about and capture people's attention and interest, while not raising any "bad" connotations (e.g., spying, invasion of privacy, attacks on other people's information systems, etc.). The chart suggests three candidate names to accomplish these ends. (Others will surely occur to the reader.)

The first one, using the term "cyberspace," has a newness to it that should capture people's attention; of the three, it provides the most vivid image of the program. The second one is less novel, but by invoking the "national information infrastructure," it draws on the momentum that concept is picking up in Washington. The third one is the most conventional and maybe the "safest," but it may not convey an adequate sense of the program's scope and importance.

---

14 "Information warfare" is obviously not a good name, at least for a program that intends to involve the civilian and non-governmental communities. It has too many bad connotations.
The CSS “Lead Agency”

Someone needs to take the lead in establishing a national CSS program

- By developing a better understanding of the cyberspace security & safety problem
  - And increasing awareness of it in relevant U.S. circles
- By developing techniques & strategies for solving the problem
  - And demonstrating elements of this family of solutions
- By serving as a catalyst
  - Stimulating the interest & involvement of other agencies & organizations

This “lead agency” will need:

- Credibility in military & civilian, and governmental & nongovernmental worlds
- An understanding of economic & social perspectives, as well as expertise in information technology

Someone needs to take the lead in establishing this national program. Whichever agency does this should have the necessary expertise in information technology. In addition, in view of the “dual” nature of the problem and the required program -- covering both military and civilian realms, and governmental and non-governmental domains, and requiring consideration of economic and social perspectives as well as technical solutions -- the “lead agency” should be capable of bridging all of these gaps and reaching out to all of these communities.\(^{15}\)

How can any “lead agency” go about taking this lead?

- By developing a better understanding of the cyberspace security and safety problem, and increasing awareness of it in relevant U.S. circles.

- By developing techniques and strategies for solving the problem, and demonstrating elements of this family of solutions.

- By serving as a catalyst, to stimulate the interest and involvement of other agencies and organizations.

\(^{15}\) In view of the broad-based nature of the problem, a group of “lead agencies” may be a more desirable solution.
The Bottom Line

- Cyberspace Security & Safety Is An Emerging National Problem
  - However big the problem is today, in 5 to 10 years it will be much bigger

- A Program Of National Scope Is Required To Adequately Address The Problem
  - Someone is needed -- a “lead agency” -- to take the initiative in developing this program

In summary, cyberspace security and safety is an emerging national problem. It is already important today, and it will be much more important tomorrow. A program of national scope -- including both military and civilian interests, both governmental and non-governmental interests, and including economic and social perspectives as well as technical solutions -- is required to address this problem.

Someone is needed to take the lead in developing this program. This “lead agency” should have the necessary expertise in information technology, and be capable of spanning the dual military/civilian, governmental/non-governmental nature of the problem and the required program.
APPENDIX. THE SPECTRUM OF CYBERSPACE SECURITY THREATS TO U.S. INTERESTS: SOME ILLUSTRATIVE EXAMPLES

Specific illustrations of security threats in cyberspace can be a helpful aid in understanding the nature and range of threats posed to U.S. interests. This appendix presents a number of such illustrative examples, which we term "case study subjects."\textsuperscript{16}

We begin with a paradigm for a generic security threat to U.S. interests in cyberspace:

An \{Actor\} mounts a computer-based attack on \{Target\} to achieve \{Objective\} using \{Instrumentalities\}.

where \{\ldots\ldots\} is a set of appropriate entities.

In this paradigm, \{Actor\}, \{Target\}, and \{Objective\} are to be viewed as inputs defining the specific threat and spanning the overall cyberspace spectrum of security threats.

Table 1 presents working lists of actors, targets, and objectives. In selecting case study subjects for illustration or analysis from this three dimensional space of Actors x Targets x Objectives, criteria to be considered include:

- **Plausibility** The case situation should be reasonable likely to occur, or at least not patently impossible.
- **Degree of Impact** The intended impact of the computer-based attack should be of significant consequence to the target, not a "pin prick."
- **Importance to Society** The case situation should be of some substantial consequence to society, not merely a "curiosity."
- **Breadth of Likely Applicability** The wider the potential applicability of instrumentalities identified in the case situation to other situations (i.e., other actors, other targets, other objectives), the better.

\textsuperscript{16} In addition to being used merely as illustrative examples, these case study subjects could also be used as the actual subjects of detailed "case studies" or "red team" efforts, systematically probing specific subsets of the information system/cyberspace spectrum to obtain a more detailed understanding of vulnerabilities and hazards.
"Advertising" Potential  Ideally, the results of the case situation should provide a useful graphic illustration of the vulnerabilities of cyberspace systems and the dangers of cyberspace "crime."

Spread of Samples across Space  The cases chosen as "points" in the three-dimensional Actors x Targets x Objectives space should span the space usefully so that different cases illustrate different vulnerabilities, points of exploitation, failure modes and architectural weaknesses.

Mindful of these criteria, and of the range of cases represented in Table 1, the nine illustrative case subjects listed in Table 2 were selected. These nine cases do a reasonably good job of spanning the space of interesting cases. Taken together, they provide a useful range of illustrations of the nature of the threats posed to U.S. interests by evil actions in cyberspace. As subjects for detailed analysis, they should provide a rich body of data on the vulnerabilities of cyberspace systems and networks, including likely points of exploitation, failure modes, and architectural weaknesses.
Table 1. The Spectrum of Actors, Targets, and Objectives

<table>
<thead>
<tr>
<th>ACTORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
</tr>
<tr>
<td>(Including criminals, hackers, zealots, and madmen)</td>
</tr>
<tr>
<td>Small, coordinated groups</td>
</tr>
<tr>
<td>(Terrorists, criminals, zealots, etc.)</td>
</tr>
<tr>
<td>Large, loosely coordinated groups</td>
</tr>
<tr>
<td>(e.g., Operation Rescue (the anti-abortion people))</td>
</tr>
<tr>
<td>Commercial Organizations</td>
</tr>
<tr>
<td>Small Countries</td>
</tr>
<tr>
<td>Large Countries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TARGETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
</tr>
<tr>
<td>Commercial Organizations</td>
</tr>
<tr>
<td>Societal Organizations</td>
</tr>
<tr>
<td>(Political, social, professional, etc.)</td>
</tr>
<tr>
<td>Physical Infrastructures</td>
</tr>
<tr>
<td>(Electric power grid, telecommunications, etc.)</td>
</tr>
<tr>
<td>Functional Infrastructures</td>
</tr>
<tr>
<td>(Financial system, etc.)</td>
</tr>
<tr>
<td>Military Organizations</td>
</tr>
<tr>
<td>Other Governmental Agencies</td>
</tr>
</tbody>
</table>

Table 1. (continued)

OBJECTIVES

To influence, harass or intimidate

For publicity

For financial gain

For revenge

To steal information, data, intellectual property, etc.

To disrupt or destroy
Table 2. Illustrative Case Subjects

1. **Individual** mounts a computer-based attack on **commercial organization** to achieve **revenge**.

   Disgruntled former employee mounts a computer attack against his former company, to get even for his dismissal.

2. **Small, coordinated group** mounts a computer-based attack on **societal organization** to achieve **disruption**.

   Fringe political group mounts a computer-based attack on a major political party during a political campaign to disrupt political process.

3. **Small, coordinated group** mounts a computer-based attack on **physical infrastructure** to achieve **disruption and intimidation**.

   Terrorist group mounts a computer-based attack on {telephone system, air traffic control system, electric power grid, etc.} to create massive disruption throughout U.S. as a means of intimidation.

4. **Small, coordinated group** mounts a computer-based attack on **functional infrastructure** to achieve **financial gain**.

   High tech criminal gang attacks banking system to steal money.

5. **Large, loosely coordinated group** mounts a computer-based attack on **individuals** to achieve **harassment, disruption and intimidation**.

   White supremists mount a computer-based attack on minority citizens living in a largely white area, to harass and intimidate them and destroy their credit ratings.
Table 2. (continued)

6. **Commercial organization** mounts a computer-based attack on **commercial organization** to achieve **theft of information and disruption**.

   Company engages in computer-based industrial espionage and disruption of the activities of a competitor, to gain an advantage during a competitive procurement.

7. **Small, coordinated group** mounts a computer-based attack on **government agency** to achieve disruption.

   Car theft ring mounts a computer-based attack on local law enforcement agency, to gain advance knowledge of police interdiction operations so that those operations can be evaded and disrupted.

8. **Small, coordinated group** mounts a computer-based attack on **military organization** to achieve disruption.

   Serbian terrorist group mounts a computer-based attack on UN peacekeeping forces, and NATO and U.S. military organizations, to disrupt UN and NATO operations in Bosnia, and to disrupt the deployment of additional U.S. forces to the area.

9. **Small country** mounts a computer-based attack on **military organization** to achieve disruption.

   Iranian agents based in Europe and North America mount a computer-based attack on U.S. military organizations, to disrupt deployment and operations of U.S. forces during crisis in the Persian Gulf.