Furthermore, as someone who wanted originally to be a marine biologist when I was in high school, had there been more programs like this funding for our national universities, who knows, I might have found a more constructive thing to do with my life.

Mr. Speaker, during consideration of this bill in the Committee on Science, I enjoyed working with my colleagues to keep Sea Grant and the Coastal Ocean Program, another marine research program, as two distinct programs with separate missions and scopes.

I would also like to recognize the sponsor of this bill, my good friend, the gentleman from Maryland (Mr. GILCHREST), and thank him for his leadership on this bill.

In closing, I urge my colleagues to support H.R. 3389.

Mr. PALLONE. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

Mr. BOEHLERT. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. CULBERSON). The question is on the motion offered by the gentleman from Utah (Mr. HANSEN) that the House suspend the rules and concur in the Senate amendment to H.R. 3389.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the Senate amendment was concurred in.

A motion to reconsider was laid on the table.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

Mr. BOEHLERT. Mr. Speaker, I move to suspend the rules and concur in the Senate amendment to the bill (H.R. 3394) an Act to authorize funding for computer and network security research and development and research fellowship programs, and for other purposes.

The Clerk read as follows:

Senate amendment:

Strike out all after the enacting clause and insert:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Security Research and Development Act''.

SEC. 2. FINDINGS.

The Congress finds the following:

(1) Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.

(2) Exponential increases in interconnectivity have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure.

(3) A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ''clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure''.

(4) Computer security technology and systems implementation lack—

(A) sufficient long term research funding;

(B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

(C) sufficient numbers of outstanding researchers in the field.

(5) Accordingly, Federal investment in computer and network security research and development must be significantly increased to—

(A) improve vulnerability assessment and technological and systems solutions;

(B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

(C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

(6) While African-Americans, Hispanics, and Native Americans constitute 25 percent of the total United States workforce and 30 percent of the college-age population, members of these minorities comprise less than 7 percent of the United States computer and information science workforce.

SEC. 3. DEFINITIONS.

In this Act:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Science Foundation.

(2) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall award grants for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security; and

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or consortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including the research areas described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and

(D) how the center will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; and

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;

(B) $24,000,000 for fiscal year 2004;

(C) $36,000,000 for fiscal year 2005;

(D) $36,000,000 for fiscal year 2006; and

(E) $36,000,000 for fiscal year 2007.

SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY PROGRAMS.

(a) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education (or consortia thereof) to establish or improve undergraduate and master's degree programs in computer and network security, to increase the number of students, including the number of students from groups historically underrepresented in these fields, who pursue undergraduate or master's degrees in fields

related to computer and network security, and to provide students with experience in government or industry related to their computer and network security studies.

(2) MERIT REVIEW.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—Grants awarded under this subsection shall be used for activities that enhance the ability of an institution of higher education (or consortium thereof) to provide high-quality undergraduate and master's degree programs in computer and network security and to recruit and retain increased numbers of students to such programs. Activities may include—

(A) revising curriculum to better prepare undergraduate and master's degree students for careers in computer and network security;

(B) establishing degree and certificate programs in computer and network security;

(C) creating opportunities for undergraduate students to participate in computer and network security research projects;

(D) acquiring equipment necessary for student instruction in computer and network security, including the installation of testbed networks for student use;

(E) providing opportunities for faculty to work with local or Federal Government agencies, private industry, nonprofit research institutions, or other academic institutions to develop new expertise or to formulate new research directions in computer and network security;

(F) establishing collaborations with other academic institutions or academic departments that seek to establish, expand, or enhance programs in computer and network security;

(G) establishing student internships in computer and network security at government agencies or in private industry;

(H) establishing collaborations with other academic institutions to establish or enhance a web-based collection of computer and network security courseware and laboratory exercises for sharing with other institutions of higher education, including community colleges;

(I) establishing or enhancing bridge programs in computer and network security between community colleges and universities; and

(J) any other activities the Director determines will accomplish the goals of this subsection.

(4) SELECTION PROCESS.—

(A) APPLICATION.—An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum—

(i) a description of the applicant's computer and network security research and instructional capacity, and in the case of an application from a consortium of institutions of higher education, a description of the role that each member will play in implementing the proposal;

(ii) a comprehensive plan by which the institution or consortium will build instructional capacity in computer and information security;

(iii) a description of relevant collaborations with government agencies or private industry that inform the instructional program in computer and network security;

(iv) a survey of the applicant's historic student enrollment and placement data in fields related to computer and network security and a study of potential enrollment and placement for students enrolled in the proposed computer and network security program; and

(v) a plan to evaluate the success of the proposed computer and network security program, including post-graduation assessment of graduate school and job placement and retention rates as well as the relevance of the instructional program to graduate study and to the workplace.

(B) AWARDS.—(i) The Director shall ensure, to the extent practicable, that grants are awarded under this subsection in a wide range of geographic areas and categories of institutions of higher education, including minority serving institutions.

(ii) The Director shall award grants under this subsection for a period not to exceed 5 years.

(5) ASSESSMENT REQUIRED.—The Director shall evaluate the program established under this subsection no later than 6 years after the establishment of the program. At a minimum, the Director shall evaluate the extent to which the program achieved its objectives of increasing the quality and quantity of students, including students from groups historically underrepresented in computer and network security related disciplines, pursuing undergraduate or master's degrees in computer and network security.

(6) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $15,000,000 for fiscal year 2003;
(B) $20,000,000 for fiscal year 2004;
(C) $20,000,000 for fiscal year 2005;
(D) $20,000,000 for fiscal year 2006; and
(E) $20,000,000 for fiscal year 2007.

(b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT OF 1992.—

(1) GRANTS.—The Director shall provide grants under the Scientific and Advanced Technology Act of 1992 (42 U.S.C. 1862i) for the purposes of section 3(a) and (b) of that Act, except that the activities supported pursuant to this subsection shall be limited to improving education in fields related to computer and network security.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $1,000,000 for fiscal year 2003;
(B) $1,250,000 for fiscal year 2004;
(C) $1,250,000 for fiscal year 2005;
(D) $1,250,000 for fiscal year 2006; and
(E) $1,250,000 for fiscal year 2007.

(c) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs for graduate students who pursue computer and network security research leading to a doctorate degree by providing funding and other assistance, and by providing graduate students with research experience in government or industry related to the students' computer and network security studies.

(2) MERIT REVIEW.—Grants shall be provided under this subsection on a merit-reviewed competitive basis.

(3) USE OF FUNDS.—An institution of higher education shall use grant funds for the purposes of—

(A) providing traineeships to students who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are pursuing research in computer or network security leading to a doctorate degree;

(B) paying tuition and fees for students receiving traineeships under subparagraph (A);

(C) establishing scientific internship programs for students receiving traineeships under subparagraph (A) in computer and network security at for-profit institutions, nonprofit research institutions, or government laboratories; and

(D) other costs associated with the administration of the program.

(4) TRAINEESHIP AMOUNT.—Traineeships provided under paragraph (3)(A) shall be in the amount of $25,000 per year, or the level of the National Science Foundation Graduate Research Fellowships, whichever is greater, for up to 3 years.

(5) SELECTION PROCESS.—An institution of higher education seeking funding under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the instructional program and research opportunities in computer and network security available to graduate students at the applicant's institution; and

(B) the internship program to be established, including the opportunities that will be made available to students for internships at for-profit institutions, nonprofit research institutions, and government laboratories.

(6) REVIEW OF APPLICATIONS.—In evaluating the applications submitted under paragraph (5), the Director shall consider—

(A) the ability of the applicant to effectively carry out the proposed program;

(B) the quality of the applicant's existing research and education programs;

(C) the likelihood that the program will recruit increased numbers of students, including students from groups historically underrepresented in computer and network security related disciplines, to pursue and earn doctorate degrees in computer and network security;

(D) the nature and quality of the internship program established through collaborations with government laboratories, nonprofit research institutions, and for-profit institutions;

(E) the integration of internship opportunities into graduate students' research; and

(F) the relevance of the proposed program to current and future computer and network security needs.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $10,000,000 for fiscal year 2003;
(B) $20,000,000 for fiscal year 2004;
(C) $20,000,000 for fiscal year 2005;
(D) $20,000,000 for fiscal year 2006; and
(E) $20,000,000 for fiscal year 2007.

(d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM SUPPORT.—Computer and network security shall be included among the fields of specialization supported by the National Science Foundation's Graduate Research Fellowships program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

(e) CYBER SECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—

(1) IN GENERAL.—The Director shall establish a program to award grants to institutions of higher education to establish traineeship programs to enable graduate students to pursue academic careers in cyber security upon completion of doctoral degrees.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) APPLICATION.—Each institution of higher education desiring to receive a grant under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director shall require.

(4) USE OF FUNDS.—Funds received by an institution of higher education under this paragraph shall—

(A) be made available to individuals on a merit-reviewed competitive basis and in accordance with the requirements established in paragraph (7);

(B) be in an amount that is sufficient to cover annual tuition and fees for doctoral study at an institution of higher education for the duration of the graduate traineeship, and shall include, in addition, an annual living stipend of $25,000; and

(C) be provided to individuals for a duration of no more than 5 years, the specific duration of each graduate traineeship to be determined by the institution of higher education, on a case-by-case basis.

(5) REPAYMENT.—Each graduate traineeship shall—

(A) subject to paragraph (5)(B), be subject to full repayment upon completion of the doctoral

degree according to a repayment schedule established and administered by the institution of higher education;

(B) be forgiven at the rate of 20 percent of the total amount of the graduate traineeship assistance received under this section for each academic year that a recipient is employed as a full-time faculty member at an institution of higher education for a period not to exceed 5 years; and

(C) be monitored by the institution of higher education receiving a grant under this subsection to ensure compliance with this subsection.

(6) EXCEPTIONS.—The Director may provide for the partial or total waiver or suspension of any service obligation or payment by an individual under this section whenever compliance by the individual is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(7) ELIGIBILITY.—To be eligible to receive a graduate traineeship under this section, an individual shall—

(A) be a citizen, national, or lawfully admitted permanent resident alien of the United States;

(B) demonstrate a commitment to a career in higher education.

(8) CONSIDERATION.—In making selections for graduate traineeships under this paragraph, an institution receiving a grant under this subsection shall consider, to the extent possible, a diverse pool of applicants whose interests are of an interdisciplinary nature, encompassing the social scientific as well as the technical dimensions of cyber security.

(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this paragraph $5,000,000 for each of fiscal years 2003 through 2007.

SEC. 6. CONSULTATION.

In carrying out sections 4 and 5, the Director shall consult with other Federal agencies.

SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COMPUTER AND NETWORK SECURITY.

Section 3(a) of the National Science Foundation Act of 1950 (42 U.S.C. 1862(a)) is amended—

(1) by striking ''and'' at the end of paragraph (6);

(2) by striking ''Congress.'' in paragraph (7) and inserting ''Congress ; and''; and

(3) by adding at the end the following:

''(8) to take a leading role in fostering and supporting research and education activities to improve the security of networked information systems.''.

SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PROGRAMS.

(a) RESEARCH PROGRAM.—The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended—

(1) by moving section 22 to the end of the Act and redesignating it as section 32;

(2) by inserting after section 21 the following new section:

''SEC. 22. RESEARCH PROGRAM ON SECURITY OF COMPUTER SYSTEMS

''(a) ESTABLISHMENT.—The Director shall establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems. The partnerships may also include government laboratories and nonprofit research institutions. The program shall—

''(1) include multidisciplinary, long-term research;

''(2) include research directed toward addressing needs identified through the activities of the Computer System Security and Privacy Advisory Board under section 20(f); and

''(3) promote the development of a robust research community working at the leading edge of knowledge in subject areas relevant to the security of computer systems by providing support for graduate students, post-doctoral researchers, and senior researchers.

''(b) FELLOWSHIPS.—

''(1) POST-DOCTORAL RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award post-doctoral research fellowships to individuals who are citizens, nationals, or lawfully admitted permanent resident aliens of the United States and are seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act.

''(2) SENIOR RESEARCH FELLOWSHIPS.—The Director is authorized to establish a program to award senior research fellowships to individuals seeking research positions at institutions, including the Institute, engaged in research activities related to the security of computer systems, including the research areas described in section 4(a)(1) of the Cyber Security Research and Development Act. Senior research fellowships shall be made available for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems.

''(3) ELIGIBILITY.—

''(A) IN GENERAL.—To be eligible for an award under this subsection, an individual shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require.

''(B) STIPENDS.—Under this subsection, the Director is authorized to provide stipends for post-doctoral research fellowships at the level of the Institute's Post Doctoral Research Fellowship Program and senior research fellowships at levels consistent with support for a faculty member in a sabbatical position.

''(c) AWARDS; APPLICATIONS.—

''(1) IN GENERAL.—The Director is authorized to award grants or cooperative agreements to institutions of higher education to carry out the program established under subsection (a). No funds made available under this section shall be made available directly to any for-profit partners.

''(2) ELIGIBILITY.—To be eligible for an award under this section, an institution of higher education shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

''(A) the number of graduate students anticipated to participate in the research project and the level of support to be provided to each;

''(B) the number of post-doctoral research positions included under the research project and the level of support to be provided to each;

''(C) the number of individuals, if any, intending to change research fields and pursue studies related to the security of computer systems to be included under the research project and the level of support to be provided to each; and

''(D) how the for-profit entities, nonprofit research institutions, and any other partners will participate in developing and carrying out the research and education agenda of the partnership.

''(d) PROGRAM OPERATION.—

''(1) MANAGEMENT.—The program established under subsection (a) shall be managed by individuals who shall have both expertise in research related to the security of computer systems and knowledge of the vulnerabilities of existing computer systems. The Director shall designate such individuals as program managers.

''(2) MANAGERS MAY BE EMPLOYEES.—Program managers designated under paragraph (1) may be new or existing employees of the Institute or individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970, except that individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 shall not directly manage such employees.

''(3) MANAGER RESPONSIBILITY.—Program managers designated under paragraph (1) shall be responsible for—

''(A) establishing and publicizing the broad research goals for the program;

''(B) soliciting applications for specific research projects to address the goals developed under subparagraph (A);

''(C) selecting research projects for support under the program from among applications submitted to the Institute, following consideration of—

''(i) the novelty and scientific and technical merit of the proposed projects;

''(ii) the demonstrated capabilities of the individual or individuals submitting the applications to successfully carry out the proposed research;

''(iii) the impact the proposed projects will have on increasing the number of computer security researchers;

''(iv) the nature of the participation by for-profit entities and the extent to which the proposed projects address the concerns of industry; and

''(v) other criteria determined by the Director, based on information specified for inclusion in applications under subsection (c); and

''(D) monitoring the progress of research projects supported under the program.

''(4) REPORTS.—The Director shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science annually on the use and responsibility of individuals on assignment at the Institute under the Intergovernmental Personnel Act of 1970 who are performing duties under subsection (d).

''(e) REVIEW OF PROGRAM.—

''(1) PERIODIC REVIEW.—The Director shall periodically review the portfolio of research awards monitored by each program manager designated in accordance with subsection (d). In conducting those reviews, the Director shall seek the advice of the Computer System Security and Privacy Advisory Board, established under section 21, on the appropriateness of the research goals and on the quality and utility of research projects managed by program managers in accordance with subsection (d).

''(2) COMPREHENSIVE 5-YEAR REVIEW.—The Director shall also contract with the National Research Council for a comprehensive review of the program established under subsection (a) during the 5th year of the program. Such review shall include an assessment of the scientific quality of the research conducted, the relevance of the research results obtained to the goals of the program established under subsection (d)(3)(A), and the progress of the program in promoting the development of a substantial academic research community working at the leading edge of knowledge in the field. The Director shall submit to Congress a report on the results of the review under this paragraph no later than 6 years after the initiation of the program.

''(f) DEFINITIONS.—In this section:

''(1) COMPUTER SYSTEM.—The term 'computer system' has the meaning given that term in section 20(d)(1).

''(2) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).''.

(b) AMENDMENT OF COMPUTER SYSTEM DEFINITION.—Section 20(d)(1)(B)(i) of National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(1)(B)(i)) is amended to read as follows:

''(i) computers and computer networks;''.

(c) CHECKLISTS FOR GOVERNMENT SYSTEMS.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology shall develop, and revise as necessary, a checklist setting forth settings and option selections that

minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal government.

(2) PRIORITIES FOR DEVELOPMENT; EXCLUDED SYSTEMS.—The Director of the National Institute of Standards and Technology may establish priorities for the development of checklists under this paragraph on the basis of the security risks associated with the use of the system, the number of agencies that use a particular system, the usefulness of the checklist to Federal agencies that are users or potential users of the system, or such other factors as the Director determines to be appropriate. The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any computer hardware or software system for which the Director of the National Institute of Standards and Technology determines that the development of a checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a checklist for the system.

(3) DISSEMINATION OF CHECKLISTS.—The Director of the National Institute of Standards and Technology shall make any checklist developed under this paragraph for any computer hardware or software system available to each Federal agency that is a user or potential user of the system.

(4) AGENCY USE REQUIREMENTS.—The development of a checklist under paragraph (1) for a computer hardware or software system does not—

(A) require any Federal agency to select the specific settings or options recommended by the checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) represent an endorsement of any such system by the Director of the National Institute of Standards and Technology; nor

(D) preclude any Federal agency from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

(d) FEDERAL AGENCY INFORMATION SECURITY PROGRAMS.—

(1) IN GENERAL.—In developing the agency-wide information security program required by section 3534(b) of title 44, United States Code, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

(2) LIMITATION.—Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 20(a)(3) of the National Institute of Standards and Technology Act (15 U.S.C.278g-3(a)(3)).

SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by adding at the end the following new subsection:

''(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.''.

SEC. 10. INTRAMURAL SECURITY RESEARCH.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended by redesignating subsection (e) as subsection (f), and by inserting after subsection (d) the following:

''(e) INTRAMURAL SECURITY RESEARCH.—As part of the research activities conducted in accordance with subsection (b)(4), the Institute shall—

''(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

''(2) carry out research associated with improving the security of real-time computing and communications systems for use in process control; and

''(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.''.

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—

(1) for activities under section 22 of the National Institute of Standards and Technology Act, as added by section 8 of this Act—

(A) $25,000,000 for fiscal year 2003;
(B) $40,000,000 for fiscal year 2004;
(C) $55,000,000 for fiscal year 2005;
(D) $70,000,000 for fiscal year 2006;
(E) $85,000,000 for fiscal year 2007; and

(2) for activities under section 20(f) of the National Institute of Standards and Technology Act, as added by section 10 of this Act—

(A) $6,000,000 for fiscal year 2003;
(B) $6,200,000 for fiscal year 2004;
(C) $6,400,000 for fiscal year 2005;
(D) $6,600,000 for fiscal year 2006; and
(E) $6,800,000 for fiscal year 2007.

SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON COMPUTER AND NETWORK SECURITY IN CRITICAL INFRASTRUCTURES.

(a) STUDY.—Not later than 3 months after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) REPORT.—The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after the date of enactment of this Act.

(c) SECURITY.—The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, $700,000.

SEC. 13. COORDINATION OF FEDERAL CYBER SECURITY RESEARCH AND DEVELOPMENT

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall coordinate the research programs authorized by this Act or pursuant to amendments made by this Act. The Director of the Office of Science and Technology Policy shall work with the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to ensure that programs authorized by this Act or pursuant to amendments made by this Act are taken into account in any government-wide cyber security research effort.

SEC. 14. OFFICE OF SPACE COMMERCIALIZATION.

Section 8(a) of the Technology Administration Act of 1998 (15 U.S.C. 1511e(a)) is amended by inserting ''the Technology Administration of'' after ''within''.

SEC. 15. TECHNICAL CORRECTION OF NATIONAL CONSTRUCTION SAFETY TEAM ACT.

Section 2(c)(1)(d) of the National Construction Safety Team Act is amended by striking ''section 8;'' and inserting ''section 7;''.

SEC. 16. GRANT ELIGIBILITY REQUIREMENTS AND COMPLIANCE WITH IMMIGRATION LAWS.

(a) IMMIGRATION STATUS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any individual who is in violation of the terms of his or her status as a nonimmigrant under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)).

(b) ALIENS FROM CERTAIN COUNTRIES.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 306(b) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1735(b)), unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

(c) NON-COMPLYING INSTITUTIONS.—No grant or fellowship may be awarded under this Act, directly or indirectly, to any institution of higher education or non-profit institution (or consortia thereof) that has—

(1) materially failed to comply with the recordkeeping and reporting requirements to receive nonimmigrant students or exchange visitor program participants under section 101(a)(15)(F), (M), or (J) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(F), (M), or (J)), or section 641 of the Illegal Immigration Reform and Responsibility Act of 1996 (8 U.S.C. 1372), as required by section 502 of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C. 1762); or

(2) been suspended or terminated pursuant to section 502(c) of the Enhanced Border Security and VISA Entry Reform Act (8 U.S.C 1762(c)).

SEC. 17. REPORT ON GRANT AND FELLOWSHIP PROGRAMS.

Within 24 months after the date of enactment of this Act, the Director, in consultation with the Assistant to the President for National Security Affairs, shall submit to Congress a report reviewing this Act to ensure that the programs and fellowships are being awarded under this Act to individuals and institutions of higher education who are in compliance with the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) in order to protect our national security.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from

New York (Mr. BOEHLERT) and the gentleman from Washington (Mr. BAIRD) each will control 20 minutes.

The Chair recognizes the gentleman from New York (Mr. BOEHLERT).

GENERAL LEAVE

Mr. BOEHLERT. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and to include extraneous material on H.R. 3394.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New York?

There was no objection.

Mr. BOEHLERT. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I am pleased to bring H.R. 3394, the Cyber Security Research and Development Act, before the House again, this time for final passage.

Back in February, the House passed the bill 400 to 12, a sign of the widely recognized need for this legislation. The Senate, by unanimous consent, has now returned the bill to us entirely intact, with a few negotiated noncontroversial additions. These additions include an additional fellowship program, greater efforts to approve the security of Federal computers, language to ensure that existing rules concerning foreign students are being enforced, and a technical correction to the bill we passed in response to the collapse of the World Trade Center.

With this background, no one should be surprised that I expect this bill to be signed shortly by the President. That is as it should be. H.R. 3394 will provide a targeted solution to a serious but largely overlooked problem: cyber security.

Cyber security is a problem that is even worse than it first appears. That is because not only are our Nation's computers and networks vulnerable to attack, and not only could a cyber attack disrupt our economy and threaten public health and safety, but we simply do not know enough about how to design computers and networks to make them less vulnerable.

For too long, cyber security has just not been a research priority. The private sector was much more focused on making computers cheaper, faster, and easier to use. The market did not put a premium on security. Government similarly turned its attention elsewhere.

As a result, computers have become omnipresent. We are more and more at their mercy, without becoming any more secure. In an age of terrorism, such willful ignorance about cyber security has got to come to an end.

□ 1430

We received yet another reminder of that monumental fact last month when the servers that run the Internet in the United States were subject to a concerted attack from overseas.

H.R. 3394 is designed quite simply, to usher in a new era in cyber security research. Cyber security research will no longer be a backwater, but rather will become a priority at two of our premier research agencies, the National Science Foundation and the National Institute of Standards and Technology, and through them, a priority in academia and industry.

And the programs created by H.R. 3394 are designed not only to spur new thinking about how to safeguard computers and networks in both the short and long run, but to make sure that we have a cadre of experts who will devote their careers to improving cyber security. The bill includes incentives for researchers to turn their attention to cyber security, and incentives to attract students to the field at the undergraduate, graduate and post-doctoral levels.

In short, this bill is a targeted but comprehensive attempt to ensure that the Nation's best minds are focused on improving cyber security. That is what it will take to stave off a cyber attack.

I want to thank the many people inside and outside Congress who helped us bring this bill to fruition. Bill Wulf, the president of the National Academy of Engineering, is really the godfather of this bill, bringing the problem and potential solutions to our attention, and he has always been available to bounce ideas off of. Industry groups have been enormously helpful and supportive, including the Information Technology Association of America and the National Association of Manufacturers.

This bill has been a bipartisan effort from its inception. I want to thank the gentleman from Texas (Mr. HALL), the ranking member, and the other Members of the minority, including the gentleman from Washington (Mr. BAIRD), who have helped shape this bill. We have had similar partnership in the other body led by Senators WYDEN and ALLEN.

In short, H.R. 3394 is a bipartisan approach to a very real but very solvable problem. I urge its final passage, not just because it is needed, but because it will reflect the fine efforts of so many dedicated people on the staff of both the Republican and Democrat side. This bill has been bicameral, and has the private sector working in partnership with government. That is the way it should be. We are addressing a very serious problem, and trying to get ahold of it before it gets out of hand, and I am optimistic we are moving in the right direction.

Mr. Speaker, I urge final passage of this bill.

Mr. Speaker, I reserve the balance of my time.

Mr. BAIRD. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong support of H.R. 3394, the Cyber Security Research and Development Act. I thank the gentleman from New York (Chairman BOEHLERT) for his outstanding leadership on this bill, and commend the gentleman from Texas (Mr. HALL) for his leadership as well.

I am tremendously honored that H.R. 3316, a computer security bill that I authored along with the gentleman from New York (Mr. BOEHLERT), are included in today's bill.

Essentially, H.R. 3394 is the same as the version that was passed by the House back in February. This legislation will address the long-term needs to secure the Nation's information infrastructure, as well as strengthening the security of the nonclassified computer systems of our Federal agencies.

Since September 11, attention has been focused in an unprecedented way on increasing our security against terrorism. Today, security has to mean more than locking doors and installing metal detectors. In addition to physical security, virtual information systems that are vital to our Nation's security and economy must be protected. Telecommunications and computer technologies are vulnerable to attack from far away by enemies who can remain anonymous, hidden in the vast maze of the Internet.

Examples of systems that rely on computer networks include our electric power grid, rail networks and financial transaction networks. The gentleman from New York (Mr. BOEHLERT) and the gentlewoman from Maryland (Mrs. MORELLA), the former chairman of the subcommittee, have had the foresight to begin hearings on this matter, even well before September 11. It is that kind of forward thinking that we need to protect our Nation's security and to secure our information infrastructure from cyber attacks.

Our vulnerability to Internet-based computer viruses, denial of service attacks, and defaced websites is well known to the general public. Such widely reported and indeed widely experienced events have increased in frequency over time. These attacks disrupt business and government activities, sometimes resulting in significant recovery costs.

While we have yet to face a catastrophic cyber attack thus far, Richard Clarke, the chair of the President's Critical Infrastructure Protection Board, has said that the government must make cyber security a priority or we face the possibility of what he termed a digital Pearl Harbor.

Potentially vulnerable computer systems are largely owned and operated by the private sector, but the government has an important role in supporting the research and development activities that provide the tools for protecting information systems. An essential component for ensuring improved information security is a vigorous and creative basic research effort focused on the security of networked information systems.

Witnesses at our Committee on Science hearings last year noted the anemic level of funding for research on computer and network security. Such lack of funding has resulted in the lack of a critical mass of researchers in the field and has severely limited the focus

of research. The witnesses at the hearings advocated increased and sustained research funding from the Federal Government to support both expanded training and research on a long-term basis.

H.R. 3394 meets those needs. It authorizes $903 million over 5 years to create new cyber security programs within the National Science Foundation and the National Institute of Standards and Technology. Under the bill, the NSF will create new cyber security research centers, undergraduate grants, community college grants, and fellowships.

The legislation also includes language I authored pertaining to NIST. The bill requires NIST to create new program grants for partnerships between academia and industry, new post-doctoral students, and a new program to encourage senior researchers in other fields to work on computer security.

I believe the legislation before us today will provide the resources necessary to ensure the security of business networks and the safety of America's computer infrastructure. I thank the staff of the Committee on Science for their tireless work on H.R. 3394, and I urge all members to support this important measure.

Mr. Speaker, I invite the chairman of the Committee on Science to enter into a brief colloquy to ask for two brief points of clarification.

Section 16(c) forbids the NSF from awarding grants or fellowships to institutions of higher education or nonprofit institutions that materially fail to comply with record-keeping requirements under certain sections of the Immigration and Nationality Act and the Illegal Immigration Reform and Responsibility Act. This section does not have an effective date at present. Many of these record-keeping requirements have yet to be written or promulgated. Therefore, the effective date for this subsection cannot be the date of enactment. In bringing the bill forward for consideration by the House, what is the gentleman's intent concerning the effective date for this provision?

Mr. BOEHLERT. Mr. Speaker, will the gentleman yield?

Mr. BAIRD. I yield to the gentleman from New York.

Mr. BOEHLERT. Mr. Speaker, the gentleman from Washington makes a very important point. Neither the Immigration and Naturalization Service nor the Department of State have provided final guidance to enable universities to participate in the new Student Exchange Visitor Information System, which provides tracking, monitoring, and access to accurate and current information on nonimmigration students and exchange visas.

It is not possible to be materially out of compliance with these requirements until the final guidance and an appropriate time for implementation have been provided to the university research community.

Mr. BAIRD. Mr. Speaker, my second question deals with Section 17 that requires the Director, 24 months after the date of enactment of this act, to submit a report to Congress reviewing this act to ensure that awards under the act are made to individuals and institutions that are in compliance with the Immigration and Nationality Act. I assume this is a simple reporting requirement similar to other reports to Congress by the NSF and that it is not meant to require the Director to enforce our Nation's immigration laws?

Mr. BOEHLERT. Mr. Speaker, if the gentleman would continue to yield, the gentleman is correct. Enforcement of the immigration laws is the responsibility of the INS and the State Department. Section 17 requires that NSF report to Congress on information it obtains from institutions of higher education, State and INS. This section does not require the NSF Director to commission a duplicative study to secure information that should be readily obtainable from the State Department and INS.

Mr. BAIRD. Mr. Speaker, I thank the gentleman for that clarification, and thank the gentleman for his leadership on this legislation.

Mr. Speaker, I reserve the balance of my time.

Mr. BOEHLERT. Mr. Speaker, I ask unanimous consent to yield the balance of my time to the gentleman from Michigan (Mr. EHLERS) for purposes of control.

The SPEAKER pro tempore (Mr. CULBERSON). Is there objection to the request of the gentleman from New York?

There was no objection.

Mr. BAIRD. Mr. Speaker, I yield 5 minutes to the gentleman from Oregon (Mr. WU).

Mr. WU. Mr. Speaker, I rise in strong support of H.R. 3394, the Cyber Security Research and Development Act. We have become increasingly reliant on the Internet and computer technology. And unfortunately, with this reliance comes increased vulnerability to cyber attacks on our network systems and infrastructure. America's network infrastructure is increasingly exposed to both benign and destructive disruptions, including defacement of web sites, denial of service, virus infections throughout the computer networks, and unauthorized intrusions and sabotage of systems and networks.

Past attacks show the types of danger and potential disruption cyber attacks can have on our Nation's infrastructure. The cyber threats to this country are significant and getting more sophisticated as time goes by.

A recent survey found that 85 percent of respondents experienced computer intrusions. Moreover, Carnegie Mellon University's CERT Coordination Center, which serves as a reporting center for Internet security problems, received almost six times the number of vulnerability reports in 2001 as it did just 2 years earlier. Similarly, the number of specific incidents reported to CERT exploded from 9.589 in 1999 to 52,658 in 2001. Even more alarming is CERT's estimates that these statistics may only represent 20 percent of the incidents that actually occurred.

The Cyber Security Research and Development Act will play a major role in fostering greater research in methods to prevent future cyber attacks and design more secure networks. This legislation will harness and link the intellectual power of the National Science Foundation, the National Institute of Science and Technology, universities, and private industry to develop new computer cryptography authentication, firewalls, forensics, intrusion detection, wireless security and systems management.

In addition, this bill is designed to draw more college undergraduate and graduate students into the field of cyber security. It establishes programs to use internships, research opportunities and better equipment to engage students in this field.

America is a leader in computer hardware and software development. In order to preserve America's technologic edge and our security, we must have a continuous pipeline of new students in computer science and research.

I strongly support this legislation and I am proud to support this important bill as it moved through the Committee on Science and again as it passed the House earlier this February. I commend the leadership of the gentleman from Washington (Mr. BAIRD), Senator WYDEN from Oregon, and the chairman of the Committee on Science, the gentleman from New York (Mr. BOEHLERT), for their leadership in moving this bill. I am confident that the Federal investment for long-term projects outlined in this legislation will enhance the security of our cyber homeland.

Mr. EHLERS. Mr. Speaker, I yield 4 minutes to the gentleman from Michigan (Mr. SMITH).

Mr. SMITH of Michigan. Mr. Speaker, I thank all Members who worked on this, but certainly commend the gentleman from Texas (Mr. HALL), the ranking member, and the gentleman from New York (Chairman BOEHLERT) for having the foresight and commitment to initiate and advance this legislation that I would suggest is very important.

As chairman of the Subcommittee on Research, I am proud to have worked on this bill and to be a prime sponsor. This act establishes programs at both the National Science Foundation and NIST, the National Institute for Standards and Technology, to advance research and, perhaps most importantly, develop a talented workforce of cyber security researchers and professionals.

While the focus in information technology has largely been to build it faster, build it smaller, and build it less expensive, perhaps now more than ever we need to know how to build it safer and more secure.

The programs authorized by this act provide much needed support for the research that will help us understand just how to do that. By supporting undergraduate and graduate post-doctoral students, as well as senior researchers who wish to focus some of their research efforts on cyber security, we will train the experts who make sure the appropriate safeguards are in place to protect us from malicious cyber attacks.

□ 1445

It is a huge challenge. It is not going to come cheaply and it is not going to come easily.

There are some unique features of this bill that will make it particularly effective in fostering innovative research and education in cyber security. For example, this act will establish a program at the National Science Foundation to help institutions of higher education purchase the equipment that they need so that students can learn how to prevent cyber attacks without risking the integrity of the college's own computer network. Another program established by this act at the National Institute of Standards and Technology will support the kind of high-risk, high-payoff research that is necessary to make great advances in cyber security but that is unlikely to get funded under the traditional peer-review process that tends to favor more conservative approaches to research questions. In addition, in recognition of the fact that effective cyber security will rely largely on the expertise of computer technicians, this bill amends the Scientific and Advanced Technology Act of 1992 to provide the National Science Foundation funding to 2-year colleges to make sure that graduates of technical programs are properly trained in cyber security.

Just a few weeks ago, an electronic attack crippled 13 computer servers that manage Internet traffic. While this hour-long attack went nearly unnoticed by routine computer users, a longer attack could cripple communication, infrastructure operations and even national security efforts. This country more than any other country in the world has come to depend on our software and our computer technology, from how we run our financial services to how we move our railroads to certainly our airlines and transportation down to how we transfer electrical power throughout the United States, not to mention our national security and our military efforts. We cannot allow these kinds of attacks to happen.

In conclusion, as we move forward in our war against terrorism, it is going to be as important for us to secure cyber space as it will be for us to secure homeland security against malicious attack. I look forward to working with the National Science Foundation as they implement the programs authorized by this act.

Mr. EHLERS. Mr. Speaker, I am pleased to yield 3 minutes to the gentleman from Texas (Mr. SMITH).

Mr. SMITH of Texas. I thank the gentleman from Michigan for yielding me this time.

Mr. Speaker, I support the Senate amendment to H.R. 3394, the Cyber Security Research and Development Act. Earlier this year, a federally funded research center operated by Carnegie Mellon University reported that breaches in security of computer systems more than doubled from 2000 to 2001. More than 52,000 incidents were reported in 2001, up from 22,000 in 2000.

Last spring the Committee on the Judiciary's Subcommittee on Crime, Terrorism and Homeland Security that I chair held a series of hearings on cyber crime. We heard testimony from local, State and Federal officials and also from the private sector. A common observation emerged: The demand for highly trained and skilled personnel to investigate computer crimes is tremendous. This problem is compounded by the rapid advances in technology which make continued training an absolute necessity. We must have training both for a new generation of cyber warriors whose most important weapon is not a gun but a laptop and for private sector companies that must protect their Internet presence.

This bill seeks to expand what many States and cities are already doing, investing in cyber security training activities. In my hometown, the University of Texas at San Antonio has established the Center for Information Assurance and Security, known as CIAS. The CIAS will be the hub of a city initiative to research, develop and address computer protection mechanisms to prevent and detect intrusions on computer networks. With funding provided in this bill, UTSA and dozens of other universities will be able to train the next generation of cyber warriors, cyber defenders and ''white hat netizens.'' This legislation supports the work at UTSA and other universities for students who want to pursue computer security studies.

While the benefits of the digital age are obvious, the Internet also has fostered an environment where hackers retrieve private data for amusement, individuals distribute software illegally, and viruses circulate with the sole purpose of debilitating computers. A well-trained and highly skilled force of cyber protectors is urgently needed in America today.

Mr. Speaker, I urge my colleagues to support this legislation.

Mr. EHLERS. Mr. Speaker, I yield myself such time as I may consume.

It is my pleasure to see this bill reach the floor for final passage and on its way to the President. I certainly agree with all the comments that have been made and I will not repeat them, but I did want to point out that in passing this legislation, both the House and the Senate have recognized the important role that the National Institute of Standards and Technology plays in cyber security. This is very important to note, because in the original proposal for the homeland security bill that particular activity would have been transferred out of the National Institute of Standards and Technology and placed in the Department of Homeland Security. I think that would have been very disruptive to the activity, but the important thing to recognize is that this group at the National Institute of Standards and Technology is the leading group in doing the basic research necessary to solve our cyber security problems. Members of the House and of the Senate working on the homeland security legislation should embrace this role as well. While there have been proposals to transfer NIST's cyber security division into the new department, this legislation clearly identifies the role that NIST should play in cyber security. As such, the proposals to move this responsibility elsewhere do not meet the test. Any conference agreement should recognize this as well by keeping NIST's cyber security division within NIST.

Let me also add that to most individuals in this land, cyber security means not having someone steal their credit card number. That is a very important function. But there is much more at stake here, as we have heard. That is the Nation's security. Two years ago, I wrote a report for the NATO parliamentary assembly, which is the legislative body relating to NATO, that discussed and studied information warfare. Much of what I said in that report is pertinent to this discussion today.

Mr. Speaker, I include that report at this point in the proceedings.

INFORMATION WARFARE AND INTERNATIONAL SECURITY

I. INTRODUCTION

1. The importance of Information Technology (IT) to the functioning of our societies is evident in virtually every human activity. Computers are involved in and often control everything from government operations to transportation, from energy to finance, from telecommunications to water management. Every day an enormous amount of information is exchanged or stored by electronic means and trillions of dollars travel throughout the world electronically. Information technology has become even more pervasive with the widespread dispersion of personal computers. According to projections of the US Computer Industry Almanac, by the year 2000 there will be more than 550 million PCs in the world, 230 million of which will be connected to the Internet (92 million in the United States alone).

2. The pace of technological change and our increasing reliance on technology are even more impressive. Five years ago, a computer chip could carry the equivalent of 1.1 million transistors. Now the number has increased to 120 million and engineers believe they can reach 400 million and even 1 billion. Capable of 256 billion multiplications per second, the latest desktop computers have acquired the speed of yesterday's supercomputers. This has accelerated the dispersion and use of the Internet. To achieve mass-user status, it took radio 35 years, television 13 years and the Internet only 4 years. Microsoft experts assert that Internet traffic doubles every 100 days and, according to other estimates, one billion people (one-sixth of humanity) will be on-line by 2005.

3. The reliance of our societies on computers and the fact that many critical infrastructures are electronically interconnected poses evident security problems. Although computer experts have been working on these problems for years, only in the mid–1990s did Western defence analysts begin to pay serious attention to them. In a variety of studies and reports, a strategic catch phrase emerged to define a new concept: Information Warfare. In a 1997 Report, the NAA Science and Technology Committee provided a first assessment of Information Warfare, analysing most of the available sources on the subject. The threat of possible attacks on information systems and the potential risks for our military and civilian infrastructures were outlined in that Report. (1)

4. In the last two years technological advances as well as governmental and international actions have changed the world of information security. As a consequence, the subject of information warfare has been extensively discussed and analysed, both within and outside the information technology and defence communities. This report analyses these new developments, starting with some new definitions of information warfare, assesses the effective strategic threats, and reports about the US and other governments' initiatives to counter them. It is also our intention to consider the concerns expressed by the science and technology community about the possible overstatement of such threats, especially with reference to some cases of media hyperbole.

II. WHAT IS INFORMATION WARFARE?

A. Definitions

5. The cited 1997 STC Report emphasised the distinction between the use of information in warfare and the newer concept of information warfare, the first being recognised since ancient times and referring basically to tactical and strategic deception, war propaganda, and destruction of command and control systems. In the current conceptualisation, information warfare ''extends far beyond the traditional battlefield, and its possible perpetrators and victims are by no means confined to the military''. A few definitions were reported then, to which your Rapporteur would like to add some new ones. The first is proposed by the Institute for the Advanced Study of Information Warfare: ''Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.'' (2)

6. The International Centre for Security Analysis of King's College, London suggests that information warfare ''is about struggles for control over information activities'' and distinguishes three levels or categories: ideational struggle for the mind of an opponent, struggle for information dominance, and attacks on, and defence of, information flows and activities. The first, highest level ''encompasses the whole range of psychological, media, diplomatic and military techniques for influencing the mind of an opponent, whether that opponent is a military commander or a whole population''. The second level could be assimilated with the Revolution in Military Affairs (RMA), whose theorists and advocates see, as the future evolution of armed forces, the goal of dominating the ''information spectrum''. The ultimate objective of this level of information warfare would be to render physical conflict ''either unnecessary or at worst short, sharp and successful''. At the third level the focus is on any kind of electronic attack upon military or civilian information infrastructures, including criminal hacking (or cracking), data disruption, illegal systems penetration, and also physical destruction, deception and psychological operations. (3)

7. The Washington based Center for Strategic and International Studies (CSIS) recently published a comprehensive study on these issues and admitted that so many different activities have been classified under the label ''information warfare'' that it is now difficult to understand exactly what it is. Nonetheless, this study classifies information warfare activities according to the source, the form, and the tactical objectives of the attack. Thus, information warfare can be viewed as a combination of these three dimensions.

8. First, an attack could originate either from outside or from within the targeted organisation or system. Second, four categories of attack can be identified:

Data attacks are conducted by inserting data into a system to make it malfunction.

Software attacks, similar to data attacks, are conducted by penetrating systems with software causing failure or making them perform functions different from those intended.

Hacking or cracking is seizing or attempting to seize control of an information system (or a vital part of it) to disrupt, deny use, steal resources or data, or cause any other kind of harm.

Physical attacks are the traditional form of attack (bombing, assaulting, and destroying) directed against information systems. An electromagnetic pulse (EMP) produced by nuclear explosions can also be included in this kind of attack.

9. All these different forms of information warfare attack can be categorised by their goals or tactical objectives: they could be aimed at exploitation, deception, disruption or destruction of information systems. (4)

10. The French Ministry of Defence has also offered an interesting definition of information warfare. It has singled out three types:

War for information (guerre pour l'information): to obtain information about the enemy's means, capabilities and strategies in order to defend ourselves;

War against information (guerre contre l'information): at the same time to protect our information systems and to disrupt or destroy the enemy's.

War through information (guerre par l'information): to conduct misinformation or deception operations against the enemy in order to achieve ''information dominance''. (5)

11. All the above are accurate and acceptable definitions, but for the sake of clarity we can try to summarise them into a simpler and more limited formula. Information warfare could be then defined as defensive and offensive operations, conducted by individuals or structured organisations with specific political and strategic goals, for the exploitation, disruption or destruction of data contained in computers or transmitted over the Internet and other networked information systems. (6)

B. Assessing the Threat

12. In general terms, a threat can be defined as the combination of a capability and a hostile intent. According to many analysts, the reason for concern about attacks upon information systems, or information warfare, is that the means of offence are widely available, inexpensive and easy to use. In a world where even governments and the military tend to rely on computer hardware and software available commercially off-the-shelf (COTS), virtually anybody with a computer and the technical skills could become a cracker or a cyberterrorist. Moreover, the progress in information technology makes the electronic tools available to conduct such attacks more sophisticated every day and, through the Internet and the interlinked computer world, easier to acquire. But the most potentially dangerous feature of information warfare is that it can be conducted from anywhere in the world and the possibilities of discovering the attack's origin, or even its presence, are extremely difficult.

13. Who can conduct such attacks? A recent analysis has listed the potential ''enemies'' according to the levels of threat. At the lower level are the crackers, or ''hackers with malicious intentions'', sometimes highly knowledgeable in technical matters and very determined, but often isolated and without a clear political agenda. Then we have some pressure groups, organisations that fight for specific political causes and might decide to acquire the technology in order to attack the information systems of other organisations or even of states. Terrorists come next in the scale: some groups are becoming increasingly sophisticated in the use of technology and can conduct strategic offensive information warfare. At the highest level are the states, many of which now have access to extremely sophisticated technology and can acquire the necessary organisational infrastructure to conduct both offensive and defensive information warfare. In fact, some experts doubt the effectiveness, capability, or even willingness of the non-state actors to conduct attacks that can seriously threaten other nations' security. (7)

14. In the last fifteen years, both the private and public sectors' information systems have been subjected to attacks that have substantially increased with the growth of the Internet. Computer viruses have been a primary concern of information security experts. These are generally very small programmes, often with destructive capabilities, designed to invade computer systems or individual PCs by attaching themselves to other bits of executable programme codes. Created by hackers, computer science students or disgruntled programmers, these viruses have been extremely destructive to many computers and networks, but have not proved to be particularly effective as weapons to date. Because of their non-professional origins, the viruses often contain errors and, moreover, their authors are often incapable of envisioning the complexity and variety of the systems they are attacking.

15. Of course, it is still possible that a state or a terrorist group can assemble a team of experts capable of creating malicious viruses and using them to conduct information warfare attacks. But computer viruses are extremely unpredictable and far from precise in their behaviour, and they might eventually damage the attacker as much as the victim. In addition, the international anti-virus industry is mature and is well positioned to create necessary antidotes to almost any new virus.

16. Other, more dangerous attacks on information systems have been conducted by criminal hacking intruders. Private corporations, particularly in the financial sector, are regularly penetrated by cybercriminals: the FBI estimates that these electronic intrusions cause yearly losses of about $10 billion in the United States alone. This is probably only the tip of the iceberg. In fact, concerns about protecting shareholder value and customer confidence may keep many firms from reporting all the attacks to law enforcement agencies.

17. Electronic intrusions into the military information infrastructure cause deep concern in the United States. According to the

CSIS, probe attacks against the Pentagon number in the tens of thousands every year. John J. Hamre, Deputy Secretary of Defense, recently stated that from January to mid-November 1998, the National Security Agency (NSA) recorded more than 3,800 incidents of intrusion attempts against the Defense Department's unclassified computer systems and networks. Over 100 of these attacks reached root-level access and many were even able to break down some kinds of service. This reflects only what has been reported to NSA, but ''the actual number of intrusions probably is considerably higher''. (8)

18. The literature and the chronicles are full of examples of successful network intrusions at the US Department of Defense (DoD) and other Western defence institutions. One of the most interesting is the break-in at the Air Force's Laboratories in the town of Rome, in New York State, when two British boys hacked into the system with the help of what is called a ''sniffer'' programme, able to capture passwords and user log-ins to the network. The case served as a learning experience for the Air Force Information Warfare Center, which then developed the advanced technical skills to counter these intrusions. Similar hacker intrusions are regularly experienced by all other US military services and government agencies.

19. While most of the attacks in the last few years were generally conducted by individuals or by small groups of intruders, with little or no political purpose, recently some cases suggested the possibility of state-sponsored hacking or cracking. Additionally, some anti-state, politically motivated activity has occurred. In October 1998, China launched a new website to publicise its efforts in human rights. A few days later, hackers replaced the home page of that site with a message condemning Beijing for its poor record in human rights. (9)

20. Another, more revealing case occurred in Ireland, where refugees from East Timor had set up a website to protest against the occupation of their country by Indonesia. The Irish Internet provider even created a new domain name ''.tp'', as if East Timor were an independent country. In January 1999, a concerted attack against the East Timorese server started, originating from 18 different places as far apart as Australia, the United States, Japan, the Netherlands and Canada. The attackers managed to render the web server useless and forced the Irish provider to disconnect its entire system. Clearly, this was not an ordinary cracker intrusion, though many doubt that the Indonesian government had the capability to conduct such a concerted information warfare action. The most probable culprit is a group of politicised hackers sympathetic with the Indonesian position. (10)

21. The NATO information system was also indirectly threatened in October 1998, when a Serbian group of hackers known as Black Hand penetrated a Kosovo Albanian web server and threatened to sabotage the Alliance's information system. The organisation temporarily closed all foreign access to its web server and its web site was down for two days. Realising that the electronic defences of the NATO web server were extremely weak, experts took some countermeasures, which proved to be insufficient in the light of subsequent events. (11)

22. During the Kosovo crisis, hackers attacked the NATO web site, causing a line saturation of the server by using a ''bombardment strategy''. The organisation had to defend itself from macro viruses from FRY trying to corrupt its e-mail system, which was also being saturated by one individual sending 2,000 messages a day. These attacks were possible because NATO was using the same server for the e-mail system and its web-pages. When these tasks are done by separate servers, as is now the case at NATO, the threat is reduced. Allied governments' web sites have also been targeted during the war, and according to US Air Force sources the attacks came not only from FRY, but also from Russia and China. It is unclear, however, whether these attacks were state-sponsored or the work of groups of hackers. Conversely, FRY's information systems were severely damaged by NATO bombings and electronic operations—although Belgrade itself dismantled communication systems to deprive its people of outside information. In addition, thousands of Western civilian hackers conducted online attacks against the FRY government's web servers. (12)

23. Such cases might not prove the existence of state-sponsored information warfare or cyberterrorism, but they offer good examples of what could happen if the capability is coupled with a hostile intent. The subsequent question is: could a group of state-sponsored terrorists or individual crackers damage the information infrastructure of another nation so as to cause a major strategic disruption? The US Department of Defense seems to think so.

24. In the summer of 1997, a simulation exercise called ''Eligible Receiver'' was conducted at the Pentagon, ordered by the Joint Chiefs of Staff, to test the ability of the nation's military and civilian infrastructure to resist a concerted information warfare attack. A team of fictional hackers, the Red Team, was allowed to use only COTS materiel and information available on the Web and had to act within the US law. So far, the results of this exercise remain strictly ''top secret''. Nonetheless, many officials have referred to it in public declarations and some have partially revealed the outcome. James Adams, a journalist based in Washington DC, claimed in a book to have interviewed senior officials about ''Eligible Receiver'': ''The [simulated] attacks focused on three main areas: the national information infrastructure, the military leadership and the political leadership. In each of these three areas, the hackers found it exceptionally easy to penetrate apparently well-defended systems. Air traffic control systems were taken down, power grids made to fail, oil refineries stopped pumping—all initially apparent incidents. At the same time, in response to a hypothetical international crisis, the Defense department was moving to deploy forces overseas and the logistics network was swinging into action. It proved remarkably easy to disrupt that network by changing orders and interrupt[ing] the logistics flow. The hackers began to feed false news reports into the decision-making process so that the politicians faced a lack of public will about prosecuting a potential conflict and lacked detailed and accurate information.'' (13)

25. In conclusion, according to Adams' sources, a team of skilled hackers, using standard equipment and publicly available information and playing by the rules, was able to cause a ''serious degradation of the Pentagon's ability to deploy and to fight''. In other words, they demonstrated that an ''electronic Pearl Harbor'' was possible.

26. Many things have changed in the last two years due to the fast pace of progress in information technology. Moreover, the policies and actions taken by the US government may have reduced the vulnerability of the nation's infrastructure. Nonetheless, if technology is helping Western governments establish better defences, it also helps potential enemies improve their capabilities to attack. A recently announced new breed of hacker software, that can learn and adapt to the network environment it attacks, may represent a new threat. According to information technology experts, the new programmes can change their mode of operation, or their targets, based on external stimulants. Pre-programmed to search for specific types of files common to most networks, such software, once in the system, can target data or files of interest to the intruders, even those marked secure or for internal use only. (14)

27. In addition, many nations are trying to acquire the capabilities needed to conduct information warfare operations and new terrorist groups like Osama bin Laden's are known to use computers and satellite telecommunications. China has recently intensified its information warfare programmes, both to protect its own military infrastructures and to enable the People's Liberation Army to conduct electronic attacks. According to James Mulvenon, a defence specialist at Rand Corporation, Beijing ''is seeking the ability both to interfere with Taiwan's command system, and ultimately to 'hack' into US military networks which control deployment in the Asian region.'' (15)

28. A serious physical threat to information systems can be posed by the effects of the electro-magnetic pulse (EMP) produced by nuclear explosions. The immediate energy release from a detonated nuclear device produces intense, rapidly varying electric and magnetic fields that can extend for considerable distances and severely affect all electronic equipment and electrical or radar transmissions even to the point of destroying equipment circuits, microprocessors, and other components. Therefore, a single, very high-altitude nuclear blast above Europe or the United States, which may cause no physical damage to structures or people, could disable or disrupt all non-hardened information systems. While few nations currently have both nuclear weapons and the missiles capable of delivering them in space, the increasing number of ''rogue'' nations with nuclear weapons that are also developing or acquiring long-range missiles may present an extremely serious EMP threat in the near future.

29. EMP effects from nuclear explosions and non-nuclear weapons, such as HERP (High-Energy Radio Frequency) guns or EMP/T (Electro-Magnetic Pulses Transformer) bombs, may be much more dangerous for civilian information systems than for military ones, most of which are now EMP hardened. Shielding of iron or other materials such as copper mesh or non-magnetic metals is generally available only for the protection of sensitive military technology.

III. RESPONSES TO THE THREAT

30. Efforts to respond to the threat of attacks to information systems, or information warfare, have been made by many nations. Generally, the military and defence ''think tanks'' have been the first to address the issue, but now most Western governments have taken steps towards more coordinated and structured responses.

31. In the United States, different panels, commissions and study groups have been examining these issues since the early 1990s and the government has taken several important measures. Congressional Committees have held hearings to investigate the nature of the information warfare threat. The National Defense University has extensively worked on the issue since the early 1990s. However, the most comprehensive appraisal of the nation's vulnerabilities in the field of information technology has been provided by the Presidential Commission on Critical Infrastructure Protection, created in 1996, involving officials from the energy, defence, commerce and law enforcement areas, as well as representatives of the private sector. After 15 months of study, the

Commission published an extensive report highlighting the vulnerabilities of the US infrastructure and the weakness of the information systems, which proved to be a potentially easy target for any concerted attack. The report also indicated that government and industry do not efficiently share information that might give warning of an electronic attack and that the federal R&D budget does not include the analysis of the threats to the information systems in the infrastructure. (16)

32. The work of the Presidential Commission resulted in the issuing in May 1998 of two Presidential Decision Directives, 62 and 63, on Critical Infrastructure Protection. The provisions of these Directives included:

Interagency co-ordination for critical infrastructure protection;

Definition of the roles and responsibilities of US agencies in fighting terrorism;

Improvements in capabilities for protecting the national information structure, the most important of which is the creation of a National Infrastructure Protection Center (NIPC) in the FBI;

Promotion of partnerships with industry and other private players to enhance computer security;

Study of plans for minimising damage and recovering rapidly from attacks to its vital infrastructures.

33. Some experts criticised the US administration decisions, claiming that the above provisions underestimated the realities of the information warfare threat. Nonetheless this is the most comprehensive and complete initiative taken so far by any Western government to respond to the risks of attacks on information systems.

34. Moreover, the DoD, actively participating in the government initiatives, has recently created a Joint Task Force for Computer Network Defense (JTF-CND) to co-ordinate all the activities in this field and direct the Pentagon's response to computer network attacks. The JTF-CND will plan defensive measures, leverage existing capabilities and develop procedures for the military commanders-in-chief, services and agencies, as well as provide strategic focus at all levels. Fully operational in the summer of 1999, the JTF-CND will also develop relationships with intelligence and law enforcement agencies, the NIPC and the private sector. (17)

35. Among European nations, France appears to have developed a coherent strategy to deal with attacks on information systems. In the absence of a general programme for infrastructure protection, such as that in the United States, the Délegation générale pour l'armement (DGA) of the Ministry of Defence has concentrated technical activities in the field of information warfare at the Centre d'électronique de l'armement (CELAR). This centre employs some 900 experts in many scientific and technological areas, and has resources and capabilities with probably no equal on the continent. All CELAR activities are related to information warfare (guerre de l'information), defensive and offensive, and are divided into five tasks: weapon systems for electronic warfare, information security, information systems, telecommunications, and electronic components. CELAR analyses the threats, establishes the needs, and tests the proficiency and the limits of the systems and equipment. In particular, within the information security field of CELAR, the Centre de l'armement pour la sécurité des systémes d'information (CASSI), is responsible for the development of all security programmes and strategies in the Ministry of Defence and acts as a consultant for other ministries and governmental agencies. (18)

36. In Germany, the efforts of the Government and the Bundestag to address the problem of security in information technology led to the creation, in 1991, of a Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, or BSI). The BSI is responsible for assessing the risks and developing the criteria, tools and procedures to assure the security of vital information systems. However, according to German officials, the BSI has concentrated its work on the non-military aspects of information warfare. In other words, it has considered the possibility of attacks to information systems only in the civilian field. At the same time, the German military has conducted some studies on information warfare and has recently initiated a new one, called ''2020'', which will consider the future evolution of the topic. Recently, a working group has been created at a federal level to draft a policy paper on ''Information Warfare and IT Security'', aimed at reaching a better co-ordination within the civilian and military fields.

37. The UK Ministry of Defence has addressed, in various areas, the problems related to information warfare, recognising that ''the potential vulnerabilities and risks arising from 'information warfare' go much wider than the Armed Forces and the defence infrastructure'' (19). The MoD is therefore known to be working with other areas of Government, allies and suppliers of key services to co-ordinate security policies and find technical solutions to protect the nation's infrastructure.

38. Other countries, such as Finland, Norway, Sweden and Switzerland have taken initiatives similar to those of the United States. Australia, Canada and Israel are investing in studies of defensive measures and approaches (20). NATO has recently analysed the threats of information warfare attacks and given indications to member states. For the moment, the most relevant studies conducted by the Alliance on the subject are classified.

IV. INFORMATION WARFARE OR SIMPLY INFORMATION SECURITY?

39. As it is often the case with extensively debated issues, some defence analysts and information security experts are doubting the actual size of the information warfare threat as it is presented by the media and even by some official reports. They contend that newspapers and magazines report stories about dangerous viruses, violated military websites and crackers penetrating corporate information systems in distorted and exaggerated ways. Some also list errors and overstatements included in official documents and defence studies. Fairness demands that we also consider these points of view, and below we summarise the most salient issues.

40. In 1997, for instance, a US government commission, that included former directors of the CIA and the National Reconnaissance Office, warned against a virus contained in an e-mail message entitled ''Penpal Greetings''. According to the commission's report, the virus ''could infect the hard-drive and destroy all data present''. Moreover, the virus was reportedly ''self-replicating'' and ''would automatically forward itself to any e-mail address stored in the recipient's in-box.'' According to many computer security analysts, the report was wrong and the Penpal virus was in fact a hoax. However, more recently several viruses spreading by e-mail could nonetheless perform extremely destructive actions. (21)

41. In March 1999, a type of macro virus propagating by e-mail called Melissa damaged, according to many journalistic sources, more than 100,000 computers. Hidden within a file of a popular word processing software, Melissa affected its security settings, rendering personal computers vulnerable to further attacks. While some defence leaders, experts on terrorism, lawmen and software executives hailed ''another warning siren of the vulnerability of our networks'' or even ''a demonstration of what an electronic Pearl Harbor might look like'', most computer security people defined Melissa as ''just another dangerous virus'', no more sophisticated than prior ones using the identical modus operandi. Moreover, they contended, Melissa (although very costly to many businesses) had no noticeable effect on Internet use or stock markets or electronic commerce. They also noted that most persons using the web on a regular basis would not open an unknown file attachment received by e-mail, especially if reportedly it contained a list of pornographic websites. (22)

42. But computer scientists and IT security experts are not only highlighting general misinformation and myths about viruses. They contest as well the alarming figures suggesting that the Pentagon and other US vital infrastructures are under almost permanent attack by crackers or cyberterrorists. They admit that malefactors can break into military and civilian web servers, and maybe even cause serious damage, but that it is far from representing an ''electronic Pearl Harbor'' for the United States. As Kevin Ziese, the computer scientist who led the Rome Laboratories investigation, and other experts put it, these break-ins can be defined as the virtual equivalent of a ''kid walking into the Pentagon cafeteria.'' (23)

43. Equating computer viruses and hacker software with weapons of mass destruction, many analysts insist, is overreaching. And classifying them as such would be like considering teen hackers or virus creators equivalent to terrorists or ''rogue'' states. The recent attacks on the Alliance's information system during the Kosovo crisis, according to these sources, might have proved just that. In fact, they report that computer security experts in the US Department of Defense were ''completely unimpressed by whatever it was Serbian hackers did during the Yugoslavian war. The worst it did is make the NATO administrator of the site work a little harder. It didn't have any impact on the Yugoslavian war at all.'' (24)

44. With regard to the supposedly frightening results of the ''Eligible Receiver'' exercise, which are still considered ''sensitive information'' by the Pentagon, many object that they should be opened up to an independent audit. Until then, computer scientists declare that they will remain extremely sceptical. Moreover, they say the Pentagon's position is in stark contrast to the wide-open discussions of computer security vulnerabilities that reign on the Internet.

45. According to William M. Arkin, an army veteran, defence analyst and editor of US Military Online, the excessive secrecy in the Pentagon's attitude towards information security reflects a basic misjudgement of the power of the Internet and the ability of the military to control it. A directive issued on 24 September 1998 by Deputy Defense Secretary John Hamre instructed all military services and agencies to ''ensure national security is not compromised or personnel placed at risk'' by information available on military websites. In fact, the Pentagon has for years had policies that required just that, and therefore only unclassified information has ever been made available on the Internet. John Pike of the Federation of American Scientists agrees with Arkin that the DoD issued this new policy out of ''a desire to show vigilance, coupled with a profound lack of understanding of information and computer security'', rather than because of

any new threats coming from the Internet. (25)

46. Many experts and scientists are critical of the approach taken by some of the Pentagon leaders not because they believe there are no threats coming from cyberspace, but because they feel those threats might have been overstated or mystified through what they call ''info-warrior rhetoric''. Computer security analysts, who have been working on these problems for years, have the impression that ''information warfare'' might just be old wine in new bottles. In fact, many of the activities now classified under this definition could be traditional intelligence work, intelligence analyses through the Internet or psychological operations and deception. For instance, the US Air Force Information Warfare Center (AFIWC, part of the Air Intelligence Agency) in San Antonio and other similar organisations are the equivalent of computer emergency response teams, and the military and civilians employed in them are all computer security specialists.

47. In spite of these reservations, it is clear that there are many serious threats. In sum, according to George Smith, editor of The Crypt Newsletter, an Internet publication dealing with computer security for computer analysts: ''It is far from proven that the country [i.e., the United States] is at the mercy of possible devastating computerized attacks. On the other hand, even the small number of examples of malicious behaviour demonstrate that computer security issues in our increasingly technological world will be of primary concern well into the foreseeable future.''

V. CONCLUSION

48. It is clear, even from the words of the most sceptical analysts, that the security of information systems must be a high priority for any nation. With the increasing dependence on information technologies, all our vital infrastructures are potentially vulnerable to some sort of external attack. Even if experts disagree on the extent and the nature of the threat, we need nonetheless to adopt measures to strengthen the protection of our information systems.

49. The first priority should be to seek objectivity in the assessment of the real threats. An independent group should be set up to provide such assessment, maybe at the international level. An example is provided by the G–8 High Tech Crime Group, a multilateral forum seeking to enhance transnational co-operation in investigating and prosecuting criminal misuse and exploitation of information systems. Parliaments and governments, as well as the industry, the scientific community and computer security experts should work within a similar group focused on information warfare threats in order to share their knowledge and competence and analyse the subject from different perspectives. A serious evaluation of the claims of computer security software and hardware producers could be the first task of such a group.

50. Programmes to raise public awareness and encourage education in the field of computer security and infrastructure protection would be extremely useful, and they should cover all possible audiences. They should include conferences, university studies, presentations at industry associations and professional societies, and sponsorship of graduate studies and programmes. In addition, research efforts are needed to both substantially improve and deploy more widely the existing technology. In particular, new capabilities for detection and identification of intrusion and improved simulation and modelling capability to understand the effects upon interconnected and interdependent infrastructures would be beneficial.

51. The law has to keep pace with the development of new technologies. Parliaments can play an important role in reconsidering and readapting the laws regulating infrastructure protection and information systems assurance. The United States can provide some good examples in terms of both statutes and case law and the Justice Department has a section devoted to this area. However, due to the open and global nature of the Internet, this effort should involve computer security experts and legislators internationally. In fact, creating a specific international set of rules or conventions is an essential prerequisite for establishing a credible and efficient Internet economy.

52. Intelligence can also contribute to a clearer understanding of the new threats of the information age in terms of actors, motives, and capabilities. Of course, the traditional intelligence work and organisation, developed during the Cold War, must be adapted to the new environment. Intelligence officials in all nations must reconsider their methods for information acquisition and rely on new sources. National agencies must also start recruiting special talents familiar with the new threats, such as skilled computer analysts with a direct experience of hacking methods.

53. Since most experts agree that commercial information systems are now more vulnerable to external attacks, it is essential to foster public-private co-operation. Much of the information that private companies need to protect their information systems may be available from the defence, intelligence and law enforcement communities. Often the private sector can better identify, understand and evaluate the threats. In many countries, co-operation between industries and their governments could be extremely helpful to share ''information and techniques related to risk management assessment, including incident reports, identification of weak spots, plans and technology to prevent attacks and disruptions, and plans for how to recover from them.'' Of course, public-private collaboration also has its limits, such as classified and secret materials or proprietary and competitively sensitive information.

54. Finally, in most Western countries, but particularly in the United States, the military should address many questions concerning the effective role of the information warfare programmes in their general policy. Programmes like those going under the definition of ''Revolution in Military Affairs'' (RMA) have already tried to assess the future impact that the use of information technology could have on weapon systems and on military organisation and strategy. However, the US military still needs to clarify its policy about the options for deterring an attack on vital information systems and the possible use of offensive information warfare. The link between information warfare and other military strategies should be better articulated: for instance, would it be possible to respond to an information warfare attack with conventional forces? Moreover, the possibility that the United States (or any other Western country) would develop and deploy offensive information warfare techniques has not been adequately discussed in public forums. This can be essential in order to build a national and possibly international consensus about the role of offensive information warfare and to clearly define its policies of use.

Notes and References

1. Lord Lyell, Lothar Ibrügger, Information Warfare and the Millennium Bomb, General Report, NAA Science and Technology Committee [AP 237 STC (97) 7]

2. Definition found on the website of the Institute for the Advanced Study of Information Warfare, self-defined ''a virtual non-governmental organisation'', http://www.psycom.net/iwar.1.html

3. Dr. Andrew Rathmell, ''Information Warfare: Implications for Arms Control'', Bulletin of Arms Control, No. 29, April 1998, on the web page of King's College London, http://www.kcl.ac.uk/orgs/icsa/cds.html. With regard to the Revolution of Military Affairs, see the STC 1998 General Report on the subject [AR 299 STC (98) 6]

4. Cybercrime-Cyberterrorism-Cyberwarfare, Averting an Electronic Waterloo, CSIS Task Force Report, Center for Strategic and International Studies, Washington DC, 1998, pp. 9–11.

5. Col Jean-Luc Moliner, ''La guerre de l'information vue par un opérationnel français'', L'Armement, No. 60, Dec. 1997–Jan. 1998, p. 11

6. Information warfare should be limited to ''specific political and strategic goals'' to avoid confusion with cybercrime or industrial espionage. Attacks to private corporations (see para.16) might be included only if conducted as part of political or strategic offensive. The limit to ''Internet and other networked information systems'' helps avoid confusion with espionage cases involving the use (or misuse) of restricted or secret information systems and/or data bases (such as recent alleged espionage at DOE weapons laboratories). Lorenzo Valeri, ''Information requirements for Information Warfare: the need for a multidisciplinary approach'', presentation prepared for the 1999 InfoWar Conference, 27 May 1999, London; and George Ballantyne, ''www.terrorism.now'', RUSI Newsbrief, April 1999, p.31. From letter by John J. Hamre published in Issues in Science and Technology, Winter 1998–99, pp.10–11

7. Alden M. Hayashi, ''The Net Effect'', Scientific American, January 1999, p. 13

8. Niall McKay, ''Indonesia, Ireland in Info War?'' Wired News, 27 January 1999, at the website http://www.wired.com/news/; Michelle Knott, ''Virtual Warfare'', New Scientist, 27 February 1999, p.51

9. Chris Nuttall, ''Kosovo info warfare spreads'', BBC Online, 1 April 1999, http://news.bbc.co.uk/ and interview with Mr. Chris Scheurweghs of the NATO Integrated Data Service

10. ''Computer hackers in Belgrade'', Aviation Week & Space Technology, 5 April 1999, p.23; Patrick Riley, ''E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight'', Fox News, 15 April 1999, http://www.foxnews.com/; Bob Brewin, ''General: Cyberattacks against NATO traced to China'', Federal Computer Week, 1 September 1999, http://www.fcw.com/

11. James Adams, The Next World War, Hutchinson, London, 1998, pp.187–8

12. George I. Seffers, ''Stealthy New Software Enhances Hacker Arsenal'', Defense News, 15 March 1999, p. 3

13. Tony Walker and Stephen Fidler, ''China studies computer warfare'', Financial Times, 16 March 1999, p. 4

14. Information on the Commission, as well as the text of the report are available on the Web at http://www.pccip.gov

15. George I. Seffers, interview with Maj. Gen. John Campbell, Defense News, 29 March 1999, p.30

16. Jean-Pierre Meunier, ''Le CELAR, centre technique de la guerre de l'information'', L'Armement, N. 60, Dec. 1997–Jan. 1998, pp.84–88

17. Strategic Defence Review, Chapter 5: The Future Shape of Our Forces, available on the Web at http://www.mod.uk/policy/sdr/

18. Andrew Rathmell, ''Information Warfare and sub-state actors'', Information, Communication & Society, Winter 1998, p. 490

19. Quoted in George Smith, ''Truth is the first casualty of cyberwar'', The Wall Street Journal, 8 September 1998

20. Kurt Kleiner, Matt Walker, ''Melissa's mayhem'', New Scientist, 10 April 1999, p.4; ''The Melissa media hangover'', The Crypt Newsletter, available on the Web at http://sun.soci.niu.edu/~crypt/

21. Quoted in George Smith, ''An Electronic Pearl Harbor? Not Likely'', Issues in Science and Technology, Fall 1998

22. David Ruppe, ''Cyber Scare'', ABC News, 4 August 1999, available on the Web at http://www.abcnews.go.com/

23. Daniel G. Dupont, ''Out of Site'', Scientific American, January 1999, p.26

24. G. Smith, ''An Electronic Pearl Harbor? Not Likely'', Issues in Science and Technology, Fall 1998

25. C. Paul Robinson, Joan B. Woodard, Samuel G. Varnado, ''Critical Infrastructure: Interlinked and Vulnerable'', Issues in Science and Technology, Fall 1998, p. 63

In summary, then, this is a very important issue, something that we must address not only for security for individuals' privacy, not only for privacy and security and integrity in business communications, but also as a means of national security. I urge a ''yes'' vote on this bill. I look forward to the President signing this bill.

Mr. Speaker, I reserve the balance of my time.

Mr. BAIRD. Mr. Speaker, I yield myself such time as I may consume.

I would like to thank the gentleman from Michigan (Mr. EHLERS) for his leadership on this issue and on so many issues on the Committee on Science. He has been one of those voices that sees problems before they present themselves to the rest of the country and has been an outstanding leader on this and many other issues.

I also want to reiterate my thanks to Chairman BOEHLERT, Ranking Member HALL, the committee staff and my own staff member, Chris Schloesser, for their good work on this.

Coincidentally, a few weeks ago I was messing around with my own computer system and I took the hardware firewall off that I have. I also have a software firewall. During a brief 15-minute period, five attacks from outside were recorded. I say that to mention that it is not just government doing its part to provide increased funds, the general public will need to increase their level of security and awareness that if they have permanent on-line connections and as broadband becomes more readily available, the general public has an important role to play because those who wish to do our country harm will try to get to our secure infrastructure through just average citizens' systems and through the network there.

I also want to underscore what the gentleman from Michigan (Mr. EHLERS) said about the cost of this legislation. It may sound expensive, and indeed it is, but the cost of a coordinated attack on our information infrastructure would be vast indeed. I would ask people to entertain the possibility of what might happen were there to be not only an attack from terrorists such as we saw on September 11 but if that were coordinated with a cyber attack on our air traffic control system or on our emergency communication systems. In an instance like that where information flow would be critical and would mean the life or death of thousands of Americans, a cyber attack would amplify exponentially the cost of a more traditional terrorist kind of attack. This money will be well spent. By spending it today, we will prepare our country for the kinds of risks we may face tomorrow.

I again urge passage of H.R. 3394. I commend those who have worked so hard to achieve this point. I thank the gentleman for his leadership.

Mr. Speaker, I yield back the balance of my time.

Mr. EHLERS. Mr. Speaker, I yield myself such time as I may consume.

In response, I want to thank the gentleman from Washington for his very perceptive comments on this issue. One important additional point to note is that the country with the most sophisticated computer systems is also the most vulnerable to information attacks and cyber attacks. Therefore, we have the most to gain by engaging in studies of cyber security to protect our extremely advanced systems.

Mr. HALL of Texas. Mr. Speaker, I rise in support of the Cyber Security Research and Development Act, H.R. 3394. The bill is substantially the same as the version which was developed in a bipartisan manner by the Science Committee and passed by the House early in the current session.

H.R. 3394 fills an important gap in current information technology research programs—namely, the need for improved security for our computers and digital communication networks.

I want to congratulate Science Committee Chairman BOEHLERT for his leadership and thank him for working with me in developing the bill.

I also want to acknowledge my colleague, Mr. BAIRD, for his important contribution to this legislation. The provisions pertaining to the National Institute of Standards and Technology originated in his bill, H.R. 3316.

Many systems that are vital to the Nation, such as transportation, the electric power grid, and financial services, rely on the transfer of information through computer networks. The trend in recent years of interconnecting computer networks has had the unintended consequence of making access to these critical systems easier for criminals, and potentially for terrorists.

As a result, there have been an increased number of assaults on network systems. Computer viruses, attacks by computer hackers, and electronic identification theft have become commonplace.

The tragic events of last year have made us realize just how vulnerable we are to attack. We are beginning to understand the critical need to protect the Nation's physical and electronic infrastructure.

Testimony before the Science Committee has highlighted a serious obstacle to achieving this goal: there are too few scientists and engineers engaged in research on information security and too little funding for security research. And as federal agencies and private industry have found, there are few people with specialized computer security skills.

H.R. 3394 establishes substantial new research programs at the National Science Foundation and the National Institute of Standards and Technology. The goal of both these multi-year programs is not only to advance computer security research, but also to expand the community of computer security researchers.

These programs will support graduate students, post-doctoral researchers, and senior researchers, while encouraging stronger ties between universities and industry. This industry linkage will provide a reality check for research priorities and will facilitate transfer of research results into new products and services.

The research and education programs at the two agencies will be reinforcing rather than duplicative. Each agency will use a different approach for the competitive review of research applications and for managing its research program. NSF and NIST have complementary linkages to the academic and industrial research communities, which will ensure a broad and varied research portfolio between the two programs.

Finally, the bill tasks the two agencies to formally coordinate their activities, and directs the Office of Science and Technology Policy to ensure that all the research activities supported under the bill are coordinated with any government-wide cyber security research effort.

Before I close, I would like to make a few comments about Sections 16 and 17, which were added to this legislation by the Senate. While I don't disagree with the objectives of these provisions, I am concerned about the procedures and the haste with which they were added to this bill. There was little consultation about the inclusion of Sec. 16 and Sec. 17 among the Members involved in drafting this legislation. In addition, there was no consultation with the university research community or the National Science Foundation, which will be affected by these provisions. The haste with which these provisions were drafted has resulted in language that is vague and unclear.

Section 16 could be interpreted as forbidding the National Science Foundation from awarding grants or fellowships to institutions of higher education or non-profit institutions that materially fail to comply with the record-keeping requirements under the Immigration and Nationality Act and the Illegal Immigration Reform and Responsibility Act. However, the record-keeping requirements for these laws have not yet been promulgated. Therefore, the effective date for this section cannot be the date of enactment. If the research performed under these grants is crucial to enhanced information security, the grants program should commence immediately; the compliance requirements should take effect only after the date of promulgation of the reporting and record-keeping requirements and after appropriate notice has been given to the affected institutions.

Section 17 requires the Director of the National Science Foundation to submit a report to Congress ensuring that awards made under this Act are given to individuals and institutions that are in compliance with the Immigration and Nationality Act. The National Science Foundation has neither the expertise nor responsibilities related to compliance with the Immigration and Nationality Act. I assume that the Department of State and the Immigration and Naturalization Service will ultimately certify compliance with the Act. Therefore, section

17 should only require the NSF report to Congress on information it obtains from State and INS. This section should not require the NSF Director to commission a duplicative study to secure information already held by State and INS.

I have discussed these issues with Chairman BOEHLERT and we are in agreement in our interpretation of these provisions and the process.

Mr. Speaker, the key to ensuring information security for the long-term is to establish a vigorous, creative and sustained basic research effort focused on the security of networked information systems. H.R. 3394 will make a major contribution toward accomplishing this goal. I commend this measure to my colleagues and ask for their support for its final passage by the House.

Mr. EHLERS. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. CULBERSON). The question is on the motion offered by the gentleman from New York (Mr. BOEHLERT) that the House suspend the rules and concur in the Senate amendment to the bill, H.R. 3394.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the Senate amendment was concurred in.

A motion to reconsider was laid on the table.

GREAT LAKES AND LAKE CHAMPLAIN ACT OF 2002

Mr. DUNCAN. Mr. Speaker, I move to suspend the rules and concur in the Senate amendments to the bill (H.R. 1070) to amend the Federal Water Pollution Control Act to authorize the Administrator of the Environmental Protection Agency to carry out projects and conduct research for remediation of sediment contamination in areas of concern in the Great Lakes, and for other purposes.

The Clerk read as follows:

Senate amendments:

Strike out all after the enacting clause and insert:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Great Lakes and Lake Champlain Act of 2002''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—GREAT LAKES

SEC. 101. SHORT TITLE.

This title may be cited as the ''Great Lakes Legacy Act of 2002''.

SEC. 102. REPORT ON REMEDIAL ACTION PLANS.

Section 118(c)(3) of the Federal Water Pollution Control Act (33 U.S.C. 1268(c)(3)) is amended by adding at the end the following:

''(E) REPORT.—Not later than 1 year after the date of enactment of this subparagraph, the Administrator shall submit to Congress a report on such actions, time periods, and resources as are necessary to fulfill the duties of the Agency relating to oversight of Remedial Action Plans under—

''(i) this paragraph; and

''(ii) the Great Lakes Water Quality Agreement.''.

SEC. 103. REMEDIATION OF SEDIMENT CONTAMINATION IN AREAS OF CONCERN IN THE GREAT LAKES.

Section 118(c) of the Federal Water Pollution Control Act (33 U.S.C. 1268(c)) is amended by adding at the end the following:

''(12) REMEDIATION OF SEDIMENT CONTAMINATION IN AREAS OF CONCERN.—

''(A) IN GENERAL.—In accordance with this paragraph, the Administrator, acting through the Program Office, may carry out projects that meet the requirements of subparagraph (B).

''(B) ELIGIBLE PROJECTS.—A project meets the requirements of this subparagraph if the project is to be carried out in an area of concern located wholly or partially in the United States and the project—

''(i) monitors or evaluates contaminated sediment;

''(ii) subject to subparagraph (D), implements a plan to remediate contaminated sediment; or

''(iii) prevents further or renewed contamination of sediment.

''(C) PRIORITY.—In selecting projects to carry out under this paragraph, the Administrator shall give priority to a project that—

''(i) constitutes remedial action for contaminated sediment;

''(ii)(I) has been identified in a Remedial Action Plan submitted under paragraph (3); and

''(II) is ready to be implemented;

''(iii) will use an innovative approach, technology, or technique that may provide greater environmental benefits, or equivalent environmental benefits at a reduced cost; or

''(iv) includes remediation to be commenced not later than 1 year after the date of receipt of funds for the project.

''(D) LIMITATION.—The Administrator may not carry out a project under this paragraph for remediation of contaminated sediments located in an area of concern—

''(i) if an evaluation of remedial alternatives for the area of concern has not been conducted, including a review of the short-term and long-term effects of the alternatives on human health and the environment; or

''(ii) if the Administrator determines that the area of concern is likely to suffer significant further or renewed contamination from existing sources of pollutants causing sediment contamination following completion of the project.

''(E) NON-FEDERAL SHARE.—

''(i) IN GENERAL.—The non-Federal share of the cost of a project carried out under this paragraph shall be at least 35 percent.

''(ii) IN-KIND CONTRIBUTIONS.—The non-Federal share of the cost of a project carried out under this paragraph may include the value of in-kind services contributed by a non-Federal sponsor.

''(iii) NON-FEDERAL SHARE.—The non-Federal share of the cost of a project carried out under this paragraph—

''(I) may include monies paid pursuant to, or the value of any in-kind service performed under, and administrative order on consent or judicial consent decree; but

''(II) may not include any funds paid pursuant to, or the value of any in-kind service performed under, a unilateral administrative order or court order.

''(iv) OPERATION AND MAINTENANCE.—The non-Federal share of the cost of the operation and maintenance of a project carried out under this paragraph shall be 100 percent.

''(F) MAINTENANCE OF EFFORT.—The Administrator may not carry out a project under this paragraph unless the non-Federal sponsor enters into such agreements with the Administrator as the Administrator may require to ensure that the non-Federal sponsor will maintain its aggregate expenditures from all other sources for remediation programs in the area of concern in which the project is located at or above the average level of such expenditures in the 2 fiscal years preceding the date on which the project is initiated.

''(G) COORDINATION.—In carrying out projects under this paragraph, the Administrator shall coordinate with the Secretary of the Army, and with the Governors of States in which the projects are located, to ensure that Federal and State assistance for remediation in areas of concern is used as efficiently as practicable.

''(H) AUTHORIZATION OF APPROPRIATIONS.—

''(i) IN GENERAL.—In addition to other amounts authorized under this section, there is authorized to be appropriated to carry out this paragraph $50,000,000 for each of fiscal years 2004 through 2008.

''(ii) AVAILABILITY.—Funds made available under clause (i) shall remain available until expended.

''(13) PUBLIC INFORMATION PROGRAM.—

''(A) IN GENERAL.—The Administrator, acting through the Program Office and in coordination with States, Indian tribes, local governments, and other entities, may carry out a public information program to provide information relating to the remediation of contaminated sediment to the public in areas of concern that are located wholly or partially in the United States.

''(B) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this paragraph $1,000,000 for each of fiscal years 2004 through 2008.''.

SEC. 104. RELATIONSHIP TO FEDERAL AND STATE AUTHORITIES.

Section 118(g) of the Federal Water Pollution Control Act (33 U.S.C. 1268(g)) is amended—

(1) by striking ''construed to affect'' and inserting the following: ''construed—

''(1) to affect'';

(2) by striking the period at the end and inserting ''or''; and

(3) by adding at the end the following:

''(2) to affect any other Federal or State authority that is being used or may be used to facilitate the cleanup and protection of the Great Lakes.''.

SEC. 105. AUTHORIZATION OF APPROPRIATIONS.

Section 118(h) of the Federal Water Pollution Control Act (33 U.S.C. 1268(h)) is amended—

(1) by striking the second sentence; and

(2) in the first sentence—

(A) by striking ''not to exceed $11,000,000'' and inserting ''not to exceed—

''(1) $11,000,000'';

(B) by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

''(2) such sums as are necessary for each of fiscal years 1992 through 2003; and

''(3) $25,000,000 for each of fiscal years 2004 through 2008.''.

SEC. 106. RESEARCH AND DEVELOPMENT PROGRAM.

(a) IN GENERAL.—In coordination with other Federal, State, and local officials, the Administrator of the Environmental Protection Agency may conduct research on the development and use of innovative approaches, technologies, and