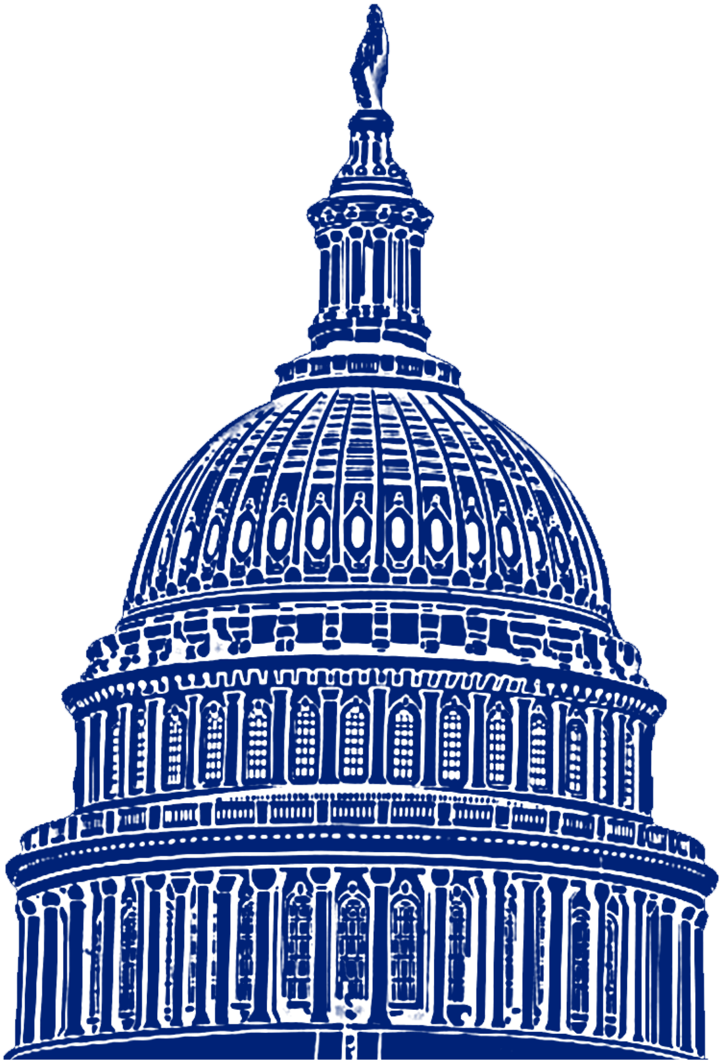


Parkland Model Congress | 2010

House Committee on Science and Technology

Topic 1: Cybersecurity

Introduction

Cybersecurity touches just about every aspect of the United States from military espionage and potential cyber sabotage of U.S. infrastructure to cyber bank thefts and loss of intellectual property. Cybersecurity has long been a priority for the federal government: Congress has passed 12 major pieces of legislation that address the issue since 1987; both the Clinton and Bush administrations instituted major cybersecurity initiatives; and the federal government is spending nearly $7 billion annually on various aspects of securing cyberspace, including research and development.

The problem is that all of our efforts and investments have not been as effective as we need them to be in improving our level of cybersecurity. Cyber crimes have cost Americans more than $8 billion over the last two years, and the threats are continuing. Cyber attacks have steadily increased over the past decade. The Pentagon reported more than 360 million attempts to break into its network last year. Earlier this month a high-profile, coordinated attack attempted — with limited success — to disrupt over two dozen government, financial and news websites in the U.S. and South Korea, including the White House.

Bloc Positions

Both parties support the cause of cybersecurity, making it an essentially bipartisan effort. The U.S. House took a tentative step toward boosting the nation's cybersecurity capabilities by passing a modest but popular bill that would fund cybersecurity research and education. The Cybersecurity Enhancement Act of 2009 (H.R. 4061), which would authorize the National Science Foundation to spend $395 million over five years on cybersecurity grants and $94 million on cybersecurity scholarships, was adopted Feb. 4. Only five House members voted against it.

"Investing in cybersecurity is the Manhattan Project of our generation," Rep. Michael Arcuri (D., N.Y.) told the House as debate on the bill began on Feb. 3. "The threat of cyber warfare cannot be overstated."

Only one Republican spoke against the bill, and her concerns focused on the rules for debating the legislation and its cost. "It's crucial that we hold the line on spending," said Rep. Virginia Foxx (R., N.C.). The Congressional Budget Office estimated that the bill would cost $639 million over the next five years.

But Rep. Arcuri tried to keep the House from being distracted by Rep. Foxx's concerns and what he called "partisan bickering." "This is a bipartisan bill that is necessary for the security of our country," he argued. "We cannot afford to maintain the status quo."

Data

Sources of Emerging Cybersecurity Threats	**Description**
Bot-network operators	Bot-network operators take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks (See Table 3 for definitions). The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or servers to relay spam or phishing attacks).

Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Types of Cyber Attacks	**Description**
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.

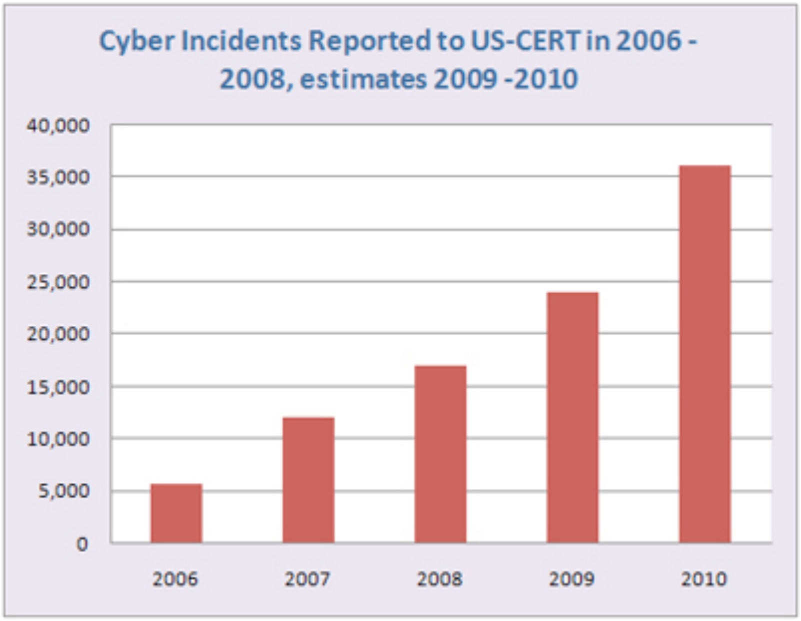
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vishing	A method of phishing based on voice-over-Internet Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

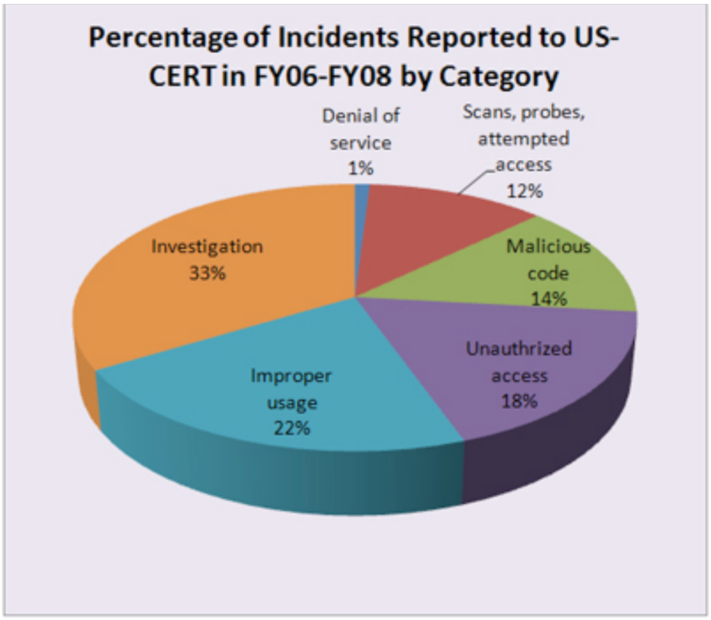
Common Types of Technology Used for Internal Monitoring	**Function**
Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.
Firewalls	Control access to and from a network or computer.
Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.
Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.

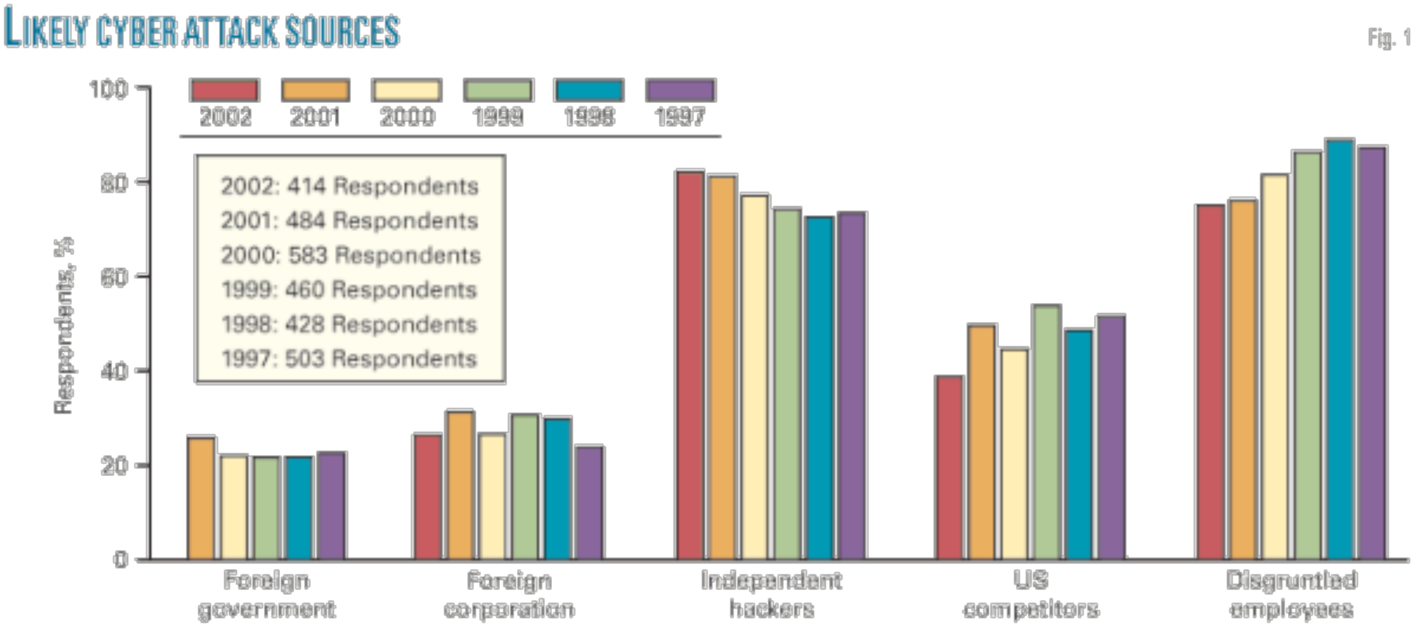
Signature-based tools — Compare files or packets to a list of "signatures"—patterns of specific files or packets that have been identified as a threat. Each signature is the unique arrangement of zeros and ones that make up the file.

Security event correlation tools — Monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred. Enable an organization to determine if ongoing system activities are operating according to its security policy.

Scanners — Analyze computers or networks for security vulnerabilities.







Source: Computer Security Institute

Topic 2: Controlling Algal Blooms

Introduction

In the United States, algae—multi- and unicellular protists—play a crucial role in marine and fresh-water ecosystems. When algae grow too quickly, however, a harmful algal bloom (HAB) can form. These visible patches of algae deplete water of oxygen (hypoxia), block sunlight, and release toxins pernicious to humans and animals. According to the National Oceanic and Atmospheric Administration (NOAA), the prevalence of HABs in the U.S. has increased. The Centers for Disease Control and Prevention (CDC) identifies several HAB-causing types of algae:

- Cyanobacteria: Toxins from this blue-green algae contaminate drinking and recreational water. Humans who drink or swim in highly cyanobacterial water may experience gastroenteritis, skin irritation, allergic responses, or liver damage.
- Harmful marine algae: These blooms occur in the ocean, producing toxins that kill fish and marine animals. Humans who ingest shellfish containing algal toxins may have neurological and gastrointestinal symptoms. Inhaling toxin-filled air associated with red tide algae may cause an asthma attack.
- Pfiesteria piscicida: This unicellular algae harms fish in estuaries. While the effects of P. piscicida on humans are not clear, humans exposed to water with high concentrations of the algae have displayed symptoms such as headache, confusion, skin rash, and eye irritation.

HABs cost the United States $82 million per year due to impacts on commercial fisheries and human health according to a conservative estimate by the NOAA. In 2002/03 alone, for example, high toxin levels from HABs resulted in a season-long closure of a Washington fishery to protect consumers from Amnesic Shellfish Poisoning (ASP). High toxin levels also caused the first commercial Dungeness crab fishery closure since 1991, decreasing revenue by $10-12 million.

In 1998, the U.S. Congress passed a law requiring the NOAA to lead an Inter-Agency Task Force on Harmful Algal Blooms and Hypoxia. The law also funded research into the origins, types and possible human health effects of HABs. In 2009 and 2010, similar bills, the Harmful Algal Blooms and Hypoxia Research and Control Amendments Acts, were passed to find a solution to the HAB crisis.

Bloc Positions

Republicans and Democrats share similar viewpoints regarding the HAB crisis. The 2009 Harmful Algal Blooms and Hypoxia Research and Control Amendment Act was passed by a bipartisan effort and co-authored by Energy and Environment Subcommittee Chairman Brian Baird, a Democrat, and Research and Science Education Subcommittee Ranking Member Vernon Ehlers, a Republican.

A red tide consumes a once pristine Florida beach.

Data

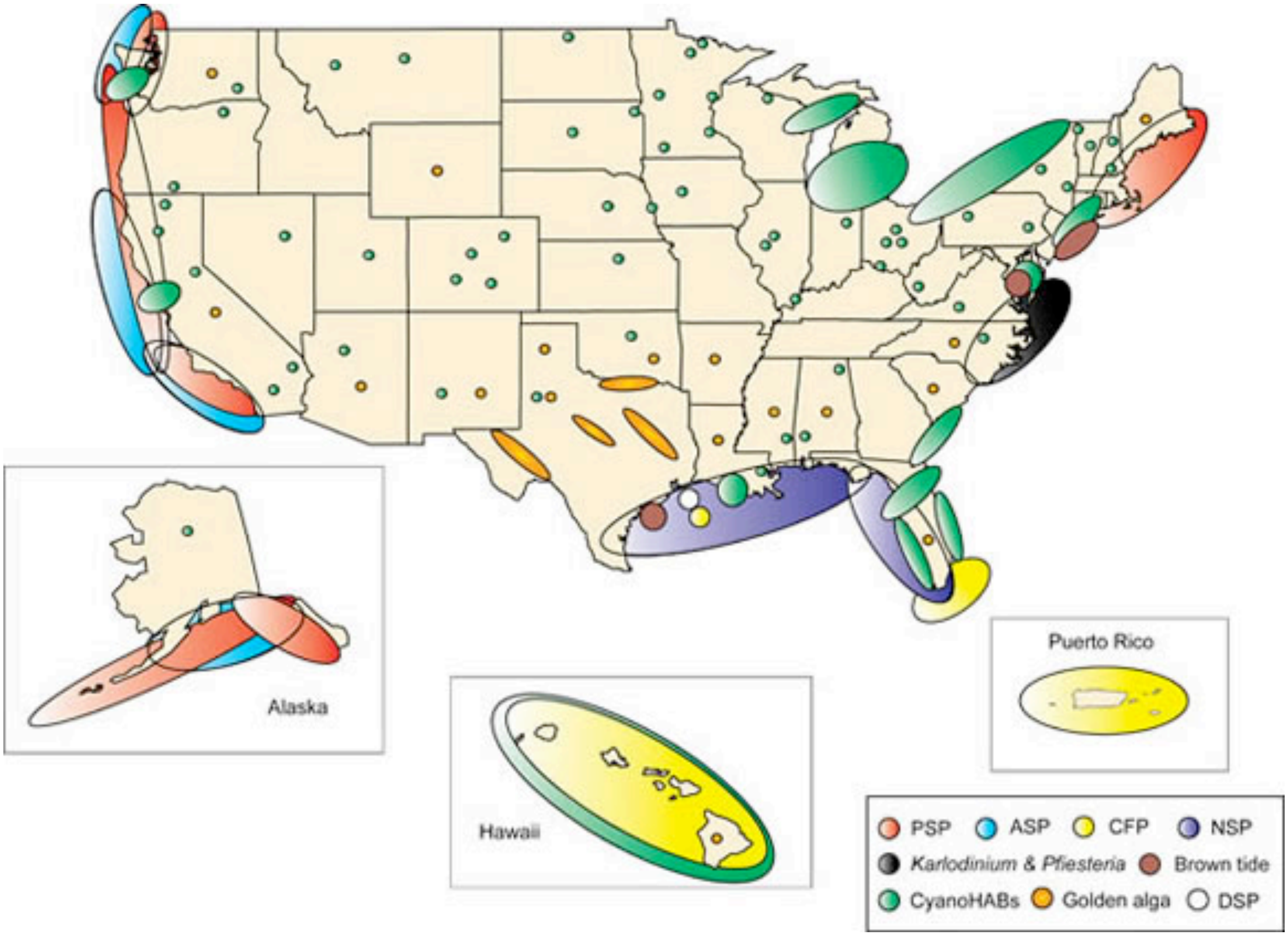


Figure 1. Distribution and Types of Algal Blooms in the U.S.
Source: U.S. National Office for Harmful Algal Blooms

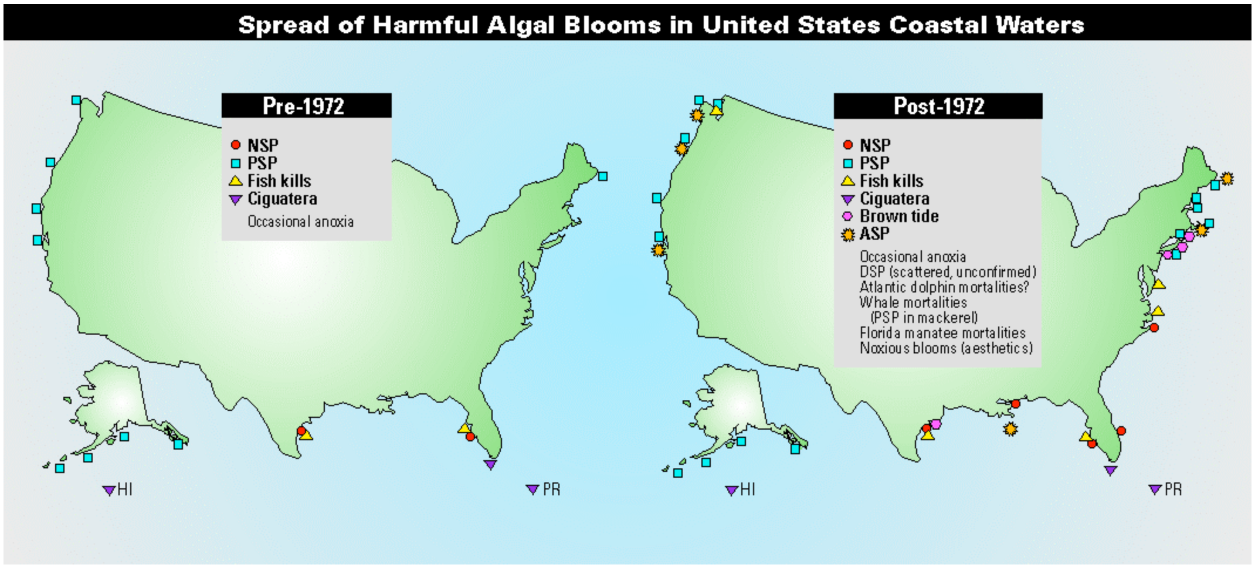

Spread of Harmful Algal Blooms in United States Coastal Waters
Pre-1972
NSP
PSP
Fish kills
Ciguatera
Occasional anoxia
HI
PR
Post-1972
NSP
PSP
Fish kills
Ciguatera
Brown tide
ASP
Occasional anoxia
DSP (scattered, unconfirmed)
Atlantic dolphin mortalities?
Whale mortalities
(PSP in mackerel)
Florida manatee mortalities
Noxious blooms (aesthetics)
HI
PR

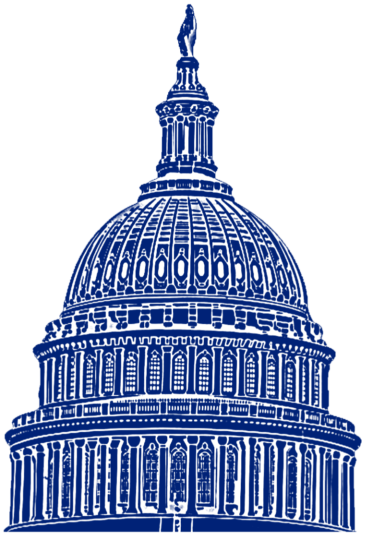
Figure 2.
Source: National Office for Marine Biotoxins and Harmful Algal Blooms

Economic Effects of HABs in the U.S. Are at Least $82 million/year*

Commercial Fisheries Impacts	$38 million/year
Public Health Costs of Illness	$37 million/year
Recreation and Tourism Impacts	$4 million/year
Coastal Monitoring and Management	$3 million/year

*2005 dollars, Hoagland and Scatasta (2006). Based on subset of outbreaks in 1987-2000.

Source: National Centers for Coastal Ocean Science



Parkland Model Congress | 2010

House Committee on Science and Technology

Eugenia Kim

Committee Co-Chair

Sophia Srinivasan

Committee Co-Chair

S. Tyler Coulton

President

Kelsey Grashoff

Vice President

Calliope Volikas

Faculty Advisor