Collegium Civitas
Foreign Policy of the United States of America

how to prevent and fight international and domestic

CYBERTERRORISM AND CYBERHOOLIGANISM

prepared by
Lukasz Jachowicz
<honey@7thGuard.net>

Warsaw, January 2003

"As we move forward in our war against terrorism, it will be as important for us to secure cyberspace as it will be for us to secure the homeland against malicious attack," (Rep. Nick Smith)

Essential Background

The Internet has evolved from a scientific and military network to a crime scene. The network is used by scientists, common users, spies and terrorists. The cost of attacks on it is rising in a fast rate, but the network is so widely used that we cannot shut it down – the communication between our agencies depends on Internet in a very big degree.

The problem is how to secure the communication and how to prevent the attacks of unauthorized Internet users to our communication channels.

Creating a new, internal only network that would replace Internet is not a good solution.
The first problem is that the cost of creating a new wide access area network would exceed the cost of protecting the existing communication channels. The second – that the new network would be less usable that Internet - it would not allow contact with the organizations and people without access to it. Of course there is a possibility of creating gateways between the both networks but it would seriously decrease the security of the internal network and make the whole operation useless.

At last, we should not forget that about 80-90% of critical technology infrastructure resides in the private sector. Even blocking unprivileged access to the government network wouldn't stop cyberterrorism.

Even if the new network is created and disconnected from the Internet, we can not forget that it would not stop attacks from real cyberterrorists – it would make them only a little bit harder. In 1997, the Department of Defense together with NSA found the power grid and 911 had serious security weaknesses. For a well educated cyberterrorist, gaining access to a non-public network is not a big problem.

Cyberterrorist is – and always will be - one step before us. There is no way to control the Internet and information about new methods of attack spread over hackers all over the world. Moreover, although we can correct most of the weaknesses in network systems, it is not possile to eliminate all of them. To prevent cyberterrorist attacks we have to join both technical and political actions.

Definitions

Cyberterrorism

Cyberterrorism is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies. (National Infrastructure Protection Center). Any attack that lead to dead, explosions or economic loss is cyberterrorism, shutting down the website of White House – is not.

There are three levels of cyberterror capability, as defined at the Naval Postgraduate School in Monterey, Ca:

1. Simple-Unstructured: the capability to conduct basic hacks against individual systems using tools created by someone else.
2. Advanced-Structured: the capability to conduct more sophisticated attacks against multiple systems and possibly to modify or create basic tools.
3. Complex-Coordinated: the capability for coordinated attacks capable of causing mass-disruption against many defense systems.

It is estimated that it would take a group of beginners 2-4 years to reach the second level, and getting to the Complex-Coordinated level takes 6 to 10 years. In case the simple group is created by people already involved in cyberterrorism, the time required to gain the third level of capabilities would be much shorter.

Cyberhooliganism

Cyberhooliganism can be defined as an criminal action against the computer system that lead to the denial of service, system destruction, website deface, stealing user's private mail etc.

Cyberhooliganism can be part of a cyberterrorist's action, can also be a job of so called script-kiddie (a person, who takes ready to use "hacking" software created by someone else and runs it against a computer system).
Cyberhooliganism is essentially nonviolent, can cause financial losses.

For example, creating the I LOVE YOU virus or destroying the NASA web page was an cyberhooliganism act.

In the following text, Cyberterrorism and Cyberhooliganism will be treated jointly.

Long-Run Actions

1. List of cyberterrorist countries

We should create a list of cyberterrorist countries, similar to Terrorist Countries List. Countries that do not sign an anti-cyberterrorism treaty and are on the top of attacking countries list should be located on Cyberterrorist Countries List (CCL).

In the end of 2002, the top ten attacking countries in terms of overall volume, according to Symantec Corp.'s report, were:

1. United States
2. South Korea
3. China
4. Germany
5. France
6. Taiwan
7. Canada
8. Italy
9. Great Britain
10. Japan

We could also use the top attacking countries per Internet capita list to create CCL. Such countries would be: South Korea, Poland, Czech Republic, France, Taiwan, Hong Kong, Belgium, Mexico, China, Israel, Iran, Kuwait, Puerto Rico, Romania, Latvia, Tanzania, Peru, Lithuania, Ecuador and Slovakia.

Most of these countries are allies of United States. Signing the anti-cyberterrorism treaty will not be a big problem for our diplomacy.

The CCL would not be used against our allies, although most of them are among both Top Attackers lists. At the moment, the CCL can be used only as an addition to other diplomatic actions.

This changes slowly as there is a very big percent rise in attacks from other countries, like Cuba (118% in second half of 2002) or Indonesia (35%). China can also get to the top of the list, as Chinese hacker groups are planning attacks on US and UK based web sites to protest war in Iraq[1].

1 *Feds: Chinese Hack Attacks Likely* by Brian Krebs, *Washington Post*, march 31, 2003.

2. International treaties

2.1 Cyber Arms Control Treaty

An international Cyber Arms Control Treaty (CACT)[2] should be created.
To be effective, it should bind all countries. It could either be forced by Cyberterrorism Countries List connected with trade restrictions or can be a part of United Nations' law system.

In cyberspace, finding an attacking person is not an easy task. An attack against a computer in one country may seem to originate from another country while perpetrated by a person in a third country that broke in to the computer in a second country to hide his or her real location. In case the second country is not bound by CACT, it may be extremely difficult to find a cyberterrorist.

The treaty should not forbid creating or using cyber arms. It would make the treaty not enforceable. Cyber arms are easy to create – in opposition to nuclear arms, no factory or special laboratory is required to create a software that can be used as a weapon. Moreover, it is sometimes impossible to find a difference between some system administration tools and cyber weapons. Advanced software used by system administrators sometimes can be used as an weapon against other computer system.

CACT should forbid using cyber weapons for criminal activity. It also should allow coordination of cyber-policeman all over the world and became the base treaty for the Cyber Police Coordination Treaty.

The CAC treaty should also force all signatories to create a domestic law that would allow prosecuting cyberterrorists for crimes committed against computer systems in other countries.

2.2. Cyber Police Coordination Treaty

Apart from the Cyber Arms Control Treaty, the Cyber Police Coordination Treaty should be created and signed by all the countries that signed CACT (or – if needed – CPCT could also became a part of United Nations' law system).
This treaty should obligate each country to create a 24/7 anti-cyberterrorist center that would help to identify and locate cyberterrorists from a given country. It also would be responsible for cooperation with similar centers in other countries. Such a center should be allowed to intercept and decrypt the communication of terrorist during the attack. Te CPCT should also allow extradition of foreign cyberterrorists to attacked countries.

2 Idea originally presented by Dorothy Denning at Arms Control in Cyberspace conference in Berlin, June 29-30, 2001.

2.3 Restrictions

Countries that do not sign anti-cyberterrorism treaty should not have any privileged status in the Department of Commerce nor any of state or government institutions. Export of advanced technology to such countries should also be restricted – especially when those countries are on the Cyberterrorist Countries List.

In case such a country is important one for our economy, we should unofficially ask it for creation the local anti-cyberterrorist center. In case such a center is created, the given state could be removed from the Cyberterrorist Countries List.

Countries that support cyberterrorism, ie. sponsor terrorists or give them special privileges, should be officially described as terrorist countries.

3. Crucial systems

Research carried out by Symantec Corp. says[3] that power and energy companies are among the most often attacked companies. That is why crucial systems, like nuclear or life-supporting devices, shouldn't be remotely controlled nor have a possibility of remote control. No computer system is completely secure and any break-in to the crucial system would be extremely harmful.

For example, in 1992, a former employee of Chevron's emergency alert network broke into company's computers and turned some systems off.

It wasn't discovered until and emergency arose at the Chevron refinery in California. The system was down for few hours and at this time, the life of thousands people in USA and Canada were at risk.

Similar situation took place in 1999, when Gazprom's (Russian gas monopoly) computer systems were attacked. Attackers gained control of central switchboard which controls gas flows in pipelines.

In 1980's, the Nuclear Regulatory Commission banned remote control of nuclear installations. More similar restrictions should be created, especially for telecommunication, transportation, financial, water supply, government, electrical power, emergency, oil and gas distribution and storage systems.

3 Symantec Internet Security Threat Report – Attack trends for Q3 and Q4, 2002

4. Open and closed source software

At the beginning of 2000, Japan's Metropolitan Police Department noticed, that some parts of software system used to track 150 police cars (including unmarked) was created by Aum Shinryko cult. All data were transmitted not only to the police systems, but also to systems owned by Aum Shinryko[4].

It wouldn't happen if the police had the source code of the tracking software.

In some countries, administration and military organizations switched from closed-source to open-source software. It is much safer – because allows fixing the security bugs quite fast - and prevents including the "Trojan horse"-like code in a system with crucial or secret data.

A lot of open-source code is available – like Linux operating system, OpenOffice office suite, encryption and communications systems and many others. Switching to the open source systems would improve security and privacy of government systems.

5. Cyber Corps

International and domestic forces should be created to fight cyberterrorism.

A special, state-sponsored, 36-months school for security experts should be created. After school, graduates would owe the state 2 years of work in anti-cyberterrorists forces. Such a school would improve the level of security in both – private and public - sectors.

Domestic forces should be coordinated with similar forces on foreign countries, so tracking down and arresting the attacker from any country would be conducted in real time, even during the attack.

Special coordination office should be created to ease the work of domestic anti-cyberterrorism forces and to exchange information about new methods of attacking and attack-detection.

Recommendation:

Options 1 and 2.3 jointly: In case cyberterrorism spreads so widely it cannot be stopped and diplomatic solutions are not effective.

Options 2.1 and 2.2 jointly: During the peace time.

Options 3, 4 and 5: Should be brought in independently.

Best option at the moment: 2.1 and 2.2 jointly.

4 Data presented by Dorothy Denning during the Congress hearing

Short-Run Actions

In case of persisting attack:

1. **Shut down communication channels to the attacking computers/networks.**

   Pros: The attack is stopped and system administrators can protect their networks against the similar attacks.

   Cons: (a) The attacker knows that he is being traced and is able to cover his tracks before anyone finds them. (b) In case of coordinated attack coming from many networks at once, big parts of the Internet can be cut of the attacked network and it may cause financial losses greater than those caused by the attack.

2. **Start tracing down the attacker, collect data about attack, do not stop the attack until enough data is collected. Cooperate with foreign system administrators and foreign anti - cyberterrorism forces in case the attack comes from third country.**

   Pros: Increased chances of tracking down the attacker. Important in case of cyberterrorism, less important in case of cyberhooliganism.

   Cons: (a) Risk of losing crucial data. (b) Sensitive information can be stolen before attacker is traced down. (c) If the system is a crucial one – like emergency or air traffic systems – the life of system-dependent users can be in danger.

3. **Remove sensitive data and conduct option 2.**

   Pros: (a) can lead to prosecution of cyberterrorist.

   Cons: (a) getting the system back to work can take long time, especially when no backup copy of lost information is made.

Recommendation:

Option 1: In case the attacked system provides secret or sensitive information that cannot be recovered in a relative short time or is a system crucial for life or economy.

Option 2: In case the attacked system is not the important one.

Option 3: In case the system can be completely recovered in a short term, or prosecuting the cyberterrorist is more important than the risk of losing data.