Special Report II: Creating a Safe, Responsible Cyber Society

In recent years, the Internet has become dramatically more user-friendly in Japan. It supports our lives as a crucial underlying structure to our society and economic activity.

On the other hand, Unauthorized Computer Access Act violation and other cybercrime violations are ever increasing. Cyberspace is being flooded with illegal and harmful information, and citizens are increasingly consulting the police on cases of online defamation and libel. With the emergence of previously unanticipated modus operandi and the extremely difficult situation of cybercrime investigation, and due to the high level of anonymity, many users have the distorted perception that "anything goes" in cyberspace, which could be reducing their respect for social norms.

The police are working hard to overcome this situation and ensure safety and security in cyberspace. In addition to cracking down on cybercrime, police need to reach a shared understanding of the current realities of cyberspace and form a ***civil cyber society that is safe, secure, and responsible***.

In order to deepen awareness of the threat of cybercrime and the importance of establishing an engaged awareness with regard to cyberspace, this special report will introduce the state of cybercrime and police efforts to combat it.

Section 1: The State of Cybercrime

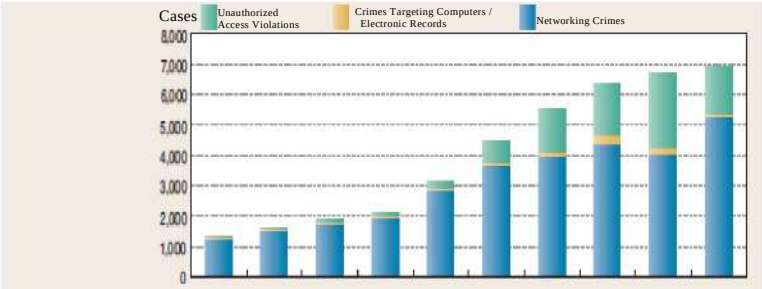
1. Overview of Cybercrime

(1) Cybercrime Cases Cleared

1) General Status of Arrests

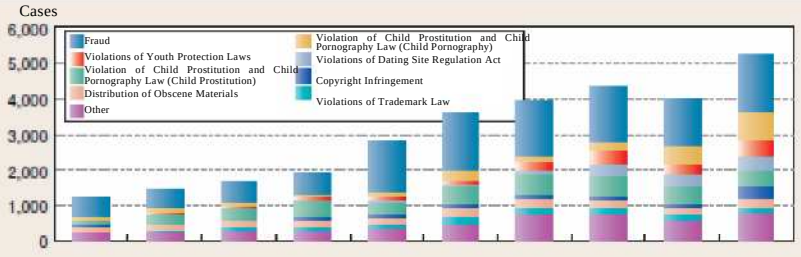
Arrests for cybercrimes are ever increasing. There were record high 6,933 cases cleared in 2010, up 243 from the previous year for a 3.6% increase. There were 5,199 cases cleared in 2010 for networking crimes—also a record high—up 1,238 from the previous year for a 31.3% increase.

Figure 1: Trends in Numbers of Cybercrimes Cleared (2001-2010)



Classification \ Year	2001	2002	2003	2004	2005	2006	2007	2008	2009	22
Total (Cases)	1,339	1,606	1,849	2,081	3,161	4,425	5,473	6,321	6,690	6,933
Unauthorized Access Violations	67	105	145	142	277	703	1,442	1,740	2,534	1,601
Crimes Targeting Computers / Electronic Records	63	30	55	55	73	129	113	247	195	133
Networking Crimes	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199

Figure 2: Trends in Numbers of Networking Crimes Cleared (2001-2010)

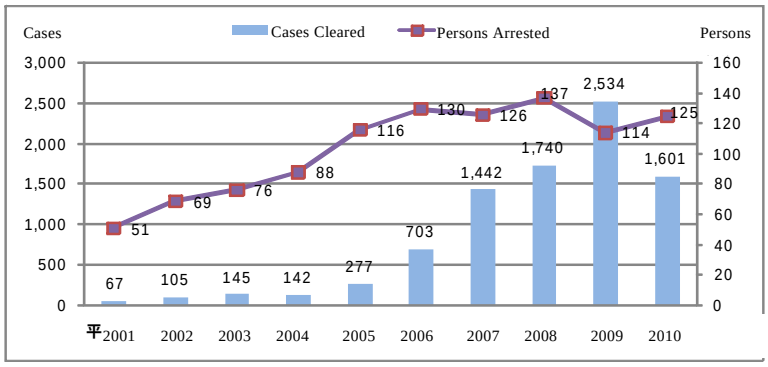


Classification / Year	2,001	2,002	2,003	2,004	2,005	2,006	2,007	2,008	2,009	2,010
Total (Cases)	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199
Fraud	485	514	521	542	1,408	1,597	1,512	1,508	1,280	1,566
Violation of Child Prostitution and Child Pornography Law (Child Pornography)	128	140	102	85	136	251	192	254	507	783
Violation of Child Prostitution and Child Pornography Law (Child Prostitution)	117	268	269	370	320	463	551	507	416	410
Violations of Dating Site Regulation Act			8	31	18	47	122	367	349	412
Violations of Youth Protection Laws	10	70	120	136	174	196	230	437	326	481
Distribution of Obscene Materials	103	109	113	121	125	192	203	177	140	218
Copyright Infringement	86	66	87	174	128	138	165	144	188	368
Violations of Trademark Law	31	37	95	82	109	218	191	192	126	119
Other	249	267	334	343	393	491	752	748	629	842

2) Unauthorized Computer Access Act Violations

There were 1,601 unauthorized access violation cases cleared in 2010, down 933 from the previous year for a decrease of 36.8%. However, this was due to one large phishing case in 2009 with 1,925 charges of unauthorized access, and arrests have exponentially risen in the past 10 years. The number of persons arrested in 2010 was 125, up 11 from the previous year for a 9.6% increase. Unauthorized access violations are still in a serious state of affairs.

Figure 3: Trends in Numbers of Unauthorized Computer Access Act Violations Cleared (2001-2010)



(2) Illegal / Harmful Information and Counseling

Of the information submitted to the Internet Hotline Center, cases classed as illegal or harmful information are steadily increasing. There were 44,683 instances in 2010, an increase of 10,715 from the previous year. Public display of obscene materials accounted for 56.7% of the counts of illegal information in 2010.

Figure 4: Trends in Cases Classed as Illegal / Harmful Information

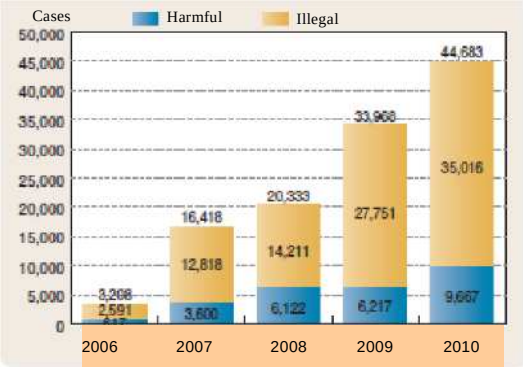
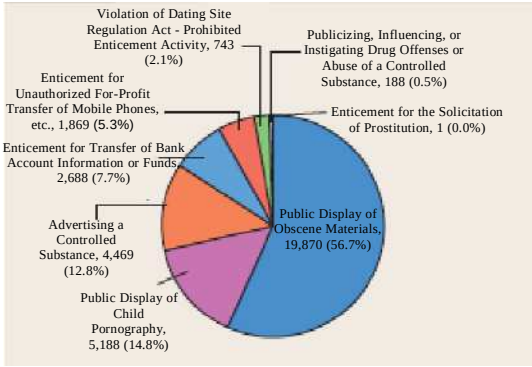
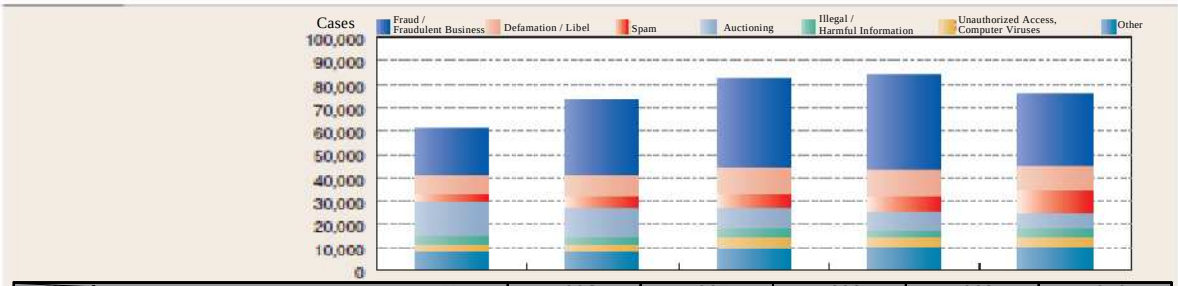


Figure 5: Breakdown of Illegal Information (2010)



Further, prefectural police counseled citizens on 75,810 cybercrime cases in 2010. This is 7,929 cases less than the previous year for a 9.5% decrease, but is still high.

Figure 6: Trends in Counseling Numbers for Cybercrime (2006-2010)



Classification \ Year	2006	2007	2008	2009	2010
Total (Cases)	61,467	73,193	81,994	83,739	75,810
Fraud / Fraudulent Business	21,020	32,824	37,794	40,315	31,333
Auctioning	14,905	12,707	8,990	7,859	6,905
Defamation / Libel	8,037	8,871	11,516	11,557	10,212
Unauthorized Access, Computer Virii	3,323	3,005	4,522	4,183	3,668
Spam	2,930	4,645	6,038	6,538	9,836
Illegal / Harmful Information	4,335	3,497	4,039	3,785	3,847
Other	6,917	7,644	9,095	9,502	10,009

(3) Issues with Cyberspace Investigations

1) Highly Anonymous, Hard to Trace

In cyberspace, you do not see the face or hear the voice of the other party, and no handwriting, fingerprints or other physical traces are left behind. Confirming whether someone is the actual party can be hard to trace when people are almost always cloaked in anonymity decided by identification codes. Given this, cybercrime investigators must identify which computer was used for the crime and clarify who was using the computer. It can be exceedingly difficult to identify suspects for cybercrimes committed from internet cafes that do not confirm user identities or ensure sufficient wireless networks security measures.

2) Few Geographical and Temporal Constraints, Prone to Short-Term Impacts on Many Unspecified Persons

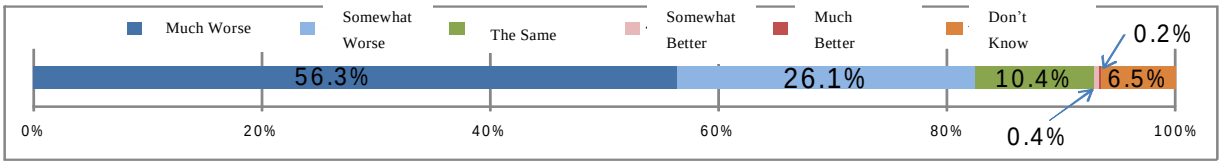
Cyberspace has few geographical or time restrictions, allowing transmission of data to an unspecified number of people at once, a great advantage to users. This also

means that when a crime is committed in cyberspace, its damage can spread nationwide. In many cybercrime investigations, it is hard to see the full picture of the damage caused; geographical relationships between details like where the crime was executed, locations of evidence, and damaged parties are tenuous. Even when connections are established, investigations often wind up spanning wide areas, including overseas, making them difficult to solve.

2. Public Awareness of Cyberspace

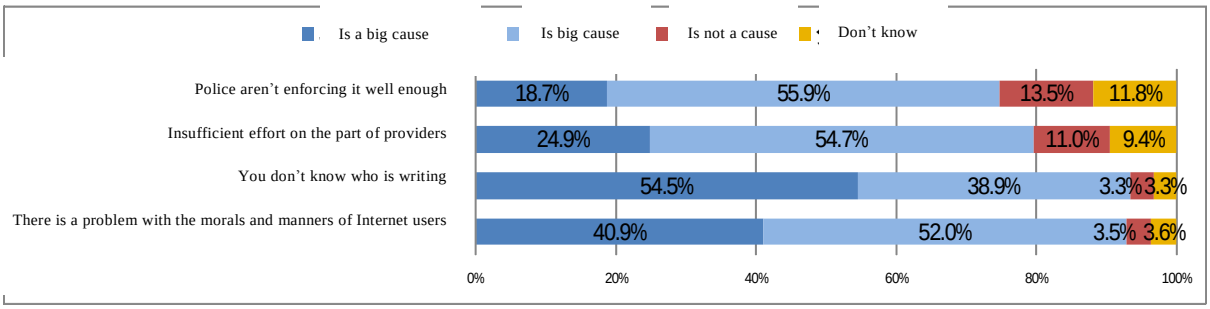
In January 2011, the NPA conducted an awareness study on Internet usage through the prefectural police. When respondents were asked to compare the morals and manners online to those in the real world, 82.4% responded that Internet morals and manners were "much worse" or "somewhat worse." From this, we infer that people are aware of their lowered morals and manners in cyberspace.

Figure 7: Comparison of Cyberspace Morals and Manners to Those in the Real World



Also, when asked the cause of the illegal and harmful information flooding the Internet, 54.5% of respondents said, "you don't know who is writing" was a "big cause," and 40.9% said, "there is a problem with the morals and manners of Internet users" was a "big cause." From this, we infer that people recognize that anonymity results in lowered morals and manners.

Figure 8: Why Illegal and Harmful Information Is Flooding the Internet



Section 2: Cybercrime Initiatives

1. Structural Developments Affecting Cybercrime Measures

(1) General Measures

1) Structural Developments

- NPA establishes Cybercrime Division (April 2004)
- Cybercrime Project established in prefectural police and info-communications departments (April 2004)
- Increase of 350 local police officers budgeted in 2011 Fiscal Budget
- New Framework for Investigation of Illegal Information introduced (trial in October 2010, scheduled to officially start July 2011)

2) Public Education and Counseling

Police are working to educate the public on cybercrime schemes and the state of illegal and harmful information online through the NPA website, public education pamphlets, and other means.

By doing so, we hope for people to become more aware of information security and improve their cyberspace morals and manners. Prefectural police have also established cybercrime counseling services to counsel people on cybercrime-related issues.

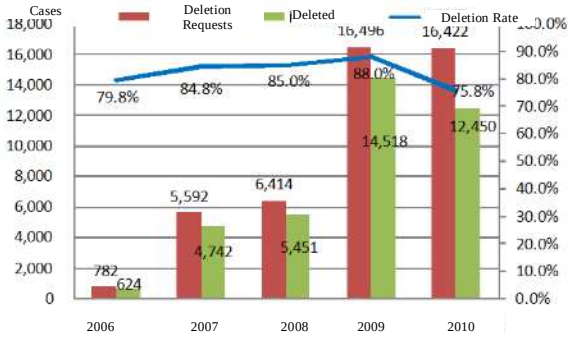
(2) Illegal / Harmful Information Measures

1) Operating the Internet Hotline Center

The NPA started operation of the Internet Hotline Center in June 2006. The center allows general Internet users to report illegal and harmful information and sends requests to website administrators and providers to delete illegal and harmful information, reported or otherwise.

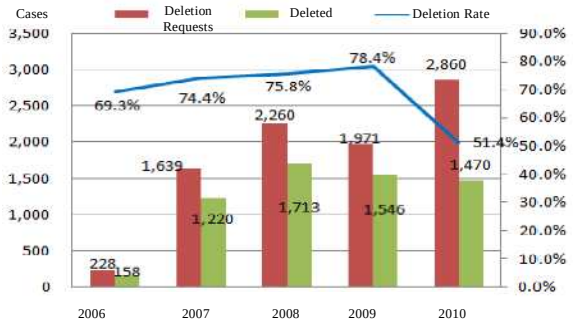
Of the 16,422 cases of illegal information in 2010 for which the center sent requests for deletion, 12,450 (75.8%) were deleted. Likewise, 1,470 (51.4%) of the 2,860 cases of harmful information were deleted. However, 3,972 (24.2%) of the cases of illegal information were not deleted despite request for deletion. Left alone, these cases will only continue to be illegal and could lead to further crimes.

Figure 9: Instances of Deleted Illegal Information (2006-2010)



Note: Numbers for 2006 from start of operation in June to December

Figure 10: Instances of Deleted Harmful Information (2006-2010)



Note: Numbers for 2006 from start of operation in June to December

2) New Framework for Investigation of Illegal Information Trial

In order to streamline investigations into illegal information, the MPD centralized investigations for determining the sources of illegal information reported to the Internet Hotline Center from October 2010. Police also started a trial run for the New Framework for Investigation of Illegal Information, by which the NPA coordinates the prefectural police to lead investigations. The system was clearly effective: 302 cases were cleared during the trial period from October 2010 to May 10, 2011, an increase of 185 over the same period the previous year. Given the success, the system is to start full operation sometime around July 2011 with an increased 350 local police officers.

2. Unauthorized Computer Access Act Violation Measures

(1) Crackdown on Unauthorized Access

1) Crackdown on Phishing Cases

Phishing scams[1] aim to acquire your personal information to obtain unauthorized access. Through the Phishing Hotline established in 2004 and other means of gathering information, police are working to detect phishing scams early and make arrests to keep the damage from spreading.

[1] Phishing occurs when a party sends an e-mail pretending to be a bank or other existing company to induce the recipient to visit a fake website made to look like the actual company website. The phisher then attempts to illegally obtain financial and personal information by prompting the recipient to enter things such as their credit card number, ID and password.

2) Protecting Against SQL Injection Attacks

SQL injection attacks [2] have become a major issue, inciting mass leaks of credit card numbers and other personal information. Police are working to crack down on unauthorized access violations through such modus operandi.

[2] SQL injection attacks exploit the SQL (Structured Query Language) programming language to illegally gain external control of a company database.

Figure 11: Overview of Phishing

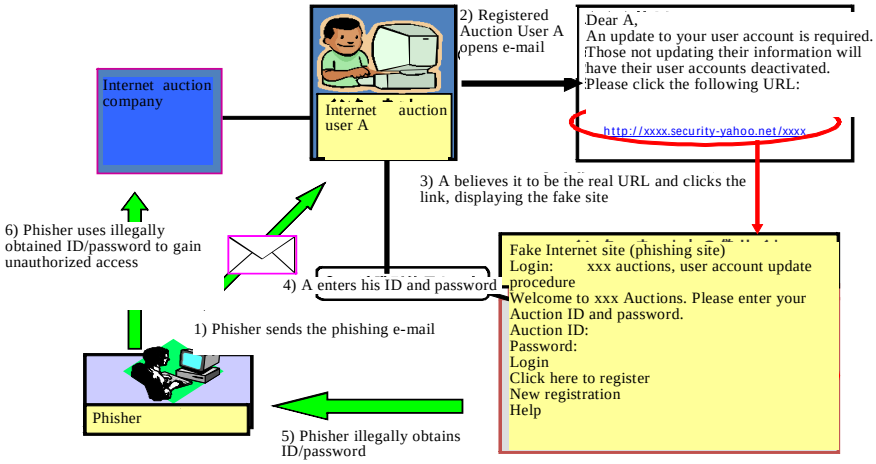
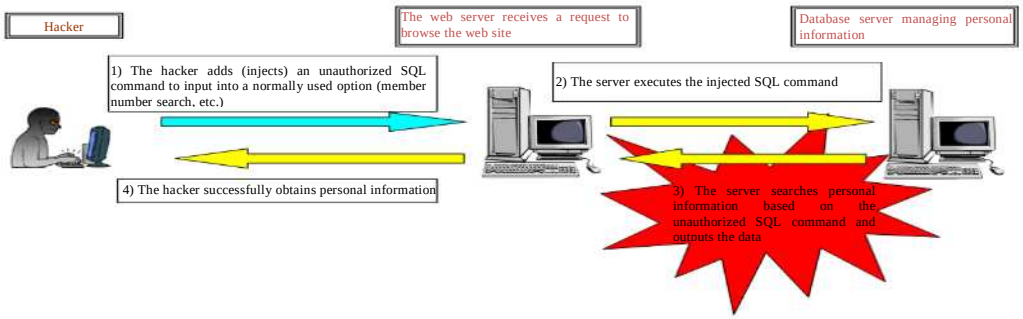


Figure 12: Overview of SQL Injection Attacks



(2) Urging Businesses to Strengthen Security Functions

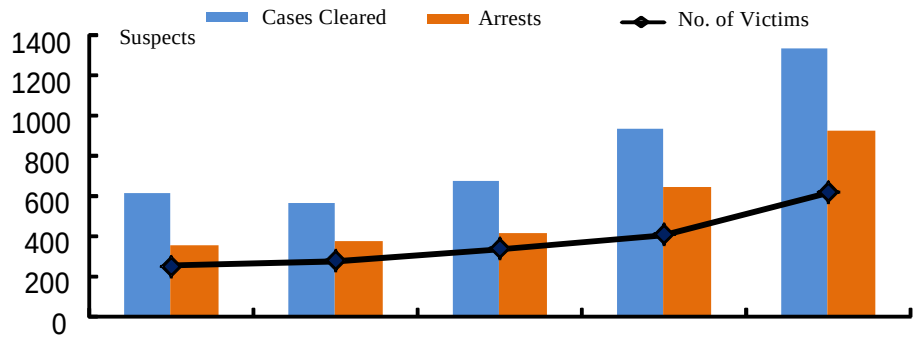
The NPA has urged businesses to strengthen their security. Based on this approach, some businesses have introduced measures such as one-time passwords.

3. Networking Crime Prevention

(1) Crackdown on Online Child Pornography

Based on the Strategic Program to Combat Child Pornography formulated by the NPA in June 2009, police have intensified enforcement of child pornography offenses online. Police are working to gather information on child pornography offenses through reports from the Internet Hotline Center, cyber patrols and other means. In light of the fact that suspects in relation to child pornography may live or perpetrate acts in far off locations and other aspects particular to Internet crimes, local prefectural police are actively conducting joint investigations.

Figure 13: Number of Child Pornography Cases Cleared (2006-2010)



Classification \ Year	2006	2007	2008	2009	2010
Cases Cleared	616	567	676	935	1,342
Cases of Internet Use	251	192	254	507	783
Arrests	350	377	412	650	926
Cases of Internet Use	174	172	213	394	644
No. of Victims	253	275	338	405	614

Case: Using file-sharing software, a civil servant (51) and others made child pornography browsable, publicly displaying it to an unspecified number of users. In September 2010, the NPA coordinated an investigation of the homes and workplaces of suspects in 50 locations nationwide with 21 prefectural police departments. Eighteen of the suspects were arrested for violating the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (public display of child pornography) and other counts.

(2) Measures Against Online Drug Trafficking

An important point of the Anti-Drug Major Reinforcement Plan, formulated by the NPA in November 2010, was the ***eradication of online drug trafficking crime***. The NPA has ramped up its collection of information on drug trafficking crimes through reports on the Internet Hotline Center, cyber patrols and other means and is promoting the use of effective investigation techniques in inherited cases to apprehend traffickers.

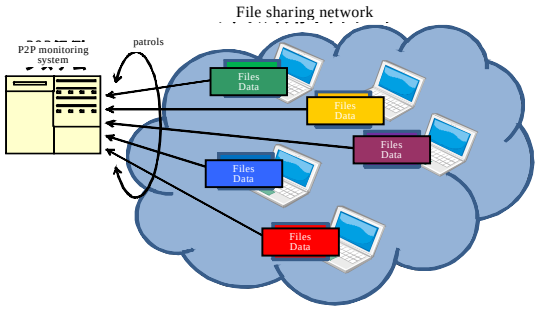
Case: An unemployed man (35) and 5 others were apprehended in April 2010 for violations of the Stimulants Control Act (joint possession, etc.) after trafficking stimulants and writing messages advertising their direct sale and mail ordering on online forums.

In addition, the administrator of the forum, a man from Hyogo (36), was aware of the postings on trafficking of stimulants and refused to either erase the posts or close the forum. He was apprehended in September 2010 for facilitating stimulant trafficking in violation of the Stimulant Control Act (assisting for-profit conveyance of stimulants).

(3) Measures Against Economic Crimes

The NPA is working hard to investigate the repurchase of illegally sold fake brand goods and pirated DVDs on Internet auction sites and round up suspects, starting with those spotted through monitoring file sharing networks with the NPA peer-to-peer (P2P) monitoring system and cyber patrols. While building connections with related agencies and groups, we are requesting website administrators to delete illegal information posted on their sites regarding economic crimes.

Figure 14: Overview of NPA P2P Monitoring System



Column: The NPA P2P Monitoring System

There are countless illegal files circulating on file sharing networks that use P2P technology to transmit data while keeping their users highly anonymous. In order to better understand how files circulate with file sharing software, the NPA started using a P2P monitoring system in 2010. The system patrols file sharing networks to gather data on files and then analyzes and searches the results.

4. Supporting Cybercrime Investigations

(1) Technical Support

Cybercrimes abuse technology in sophisticated manners, and controlling them is increasingly requiring advanced technical knowledge. The NPA is establishing a system to handle these needs, establishing a High-Tech Crime Technology Division in the Info-Communications Bureau of the NPA, Regional Police Bureaus, and prefectural police.

Using its P2P monitoring system, the NPA also takes measures such as providing useful information to investigations on violations of the Copyright Act, Child Prostitution and Child Pornography Act and other laws using file-sharing software.

12th Interpol Asia-South Pacific Working Party on Information Technology Crime

(2) International Cooperation

Cybercrimes pass international borders with ease. The NPA is actively working on projects to combat international cybercrimes through international conferences such as the G8 Roma/Lyon High-Tech Crime Subgroup and ICPO Asia-South Pacific Working Party on IT Crime, and also through cooperation with foreign investigation agencies.

Furthermore, with the globalization of crime, an increasing number of cases involve exploitation of foreign-made electronic devices. In order to extract and analyze the data saved on such devices, police need to understand the latest in foreign technologies, share information with foreign security organizations, and increase analytical capabilities. The NPA promotes international ties through initiatives such as hosting the Asian Regional Cybercrime Investigation Technology Conference and developing and operating the Cybercrime Technology Information Network System.

5. Promoting Voluntary and Independent Action by Businesses

(1) Comprehensive Security Measures Conference

Dealing properly with cybercrime requires the use of advanced technology. In addition to police enforcement, we also need voluntary, independent action by businesses and other public-private partnerships. Therefore, the NPA hosts the Comprehensive Security Measures Conference to ensure the safety and reliability of telecommunications networks and studies the state of cooperation between the industries and the government on information security.

The Comprehensive Security Measures Conference has resulted in the proposal that started operation of the Internet Hotline Center, and, in June 2009, also prompted the start of the Council on the Prevention of the Spread of Child Pornography.

The theme of the 2010 conference was creating a safe, secure, and responsible cyber society. In it, participants discussed the following: 1) measures against unauthorized access, 2) measures against illegal and harmful information, and 3) training cybercrime prevention volunteers.

The following proposals were made for each point.

1) Measures against unauthorized access:

Prevention measures for phishing and SQL injection attacks, and building a support framework urging private businesses to independently upgrade their access control functions

2) Measures against illegal and harmful information:

Spurring more people to report to the Internet Hotline Center and arresting pernicious site administrators who ignore requests to delete illegal information

3)Training cybercrime prevention volunteers:

Organizing training by developing guidelines

(2) Measures for Social Networking and Forum Sites

In 2010, 1,239 children were victims of crimes resulting from use of social networking sites and public forums. This is an increase of 103 over last year and the third increase in as many years. The NPA is therefore pushing forward with several measures. These measures include requests to the companies of social networking sites with high numbers of victimized children to construct sufficient systems scaled to its user base, including content checks for private messages.

Column: Aiming for 100% Content Filtering

Use of content filtering for mobile phones is an effective means of preventing children from browsing information that is harmful to youths when going online via their mobile phones.

According to study results released by the Cabinet Office in February 2011, 77.6% of elementary school students, 67.1% of middle school students and 49.3% of high school students use content filters. Meanwhile, more than 90% of child victims of crimes on social networking sites in the first half of 2010 were not using content filters.

In cooperation with relevant ministries, the police are striving for a 100% usage rate for content filters to prevent children from falling victim to these crimes. In particular, sites selling and issuing contracts for mobile phones are seen as the front line in terms of urging phone users to use content filters. Police are therefore enhancing requests to businesses handling mobile phones, including phone distributors and retail electronics stores, to explain the importance of filtering content to parents and guardians where phones are bought and contracted, and to recommend

safer content filtering services to all their customers.

Police are also promoting various public awareness activities, such as working to raise parental awareness on content filters at orientation and other parent-teacher meetings.

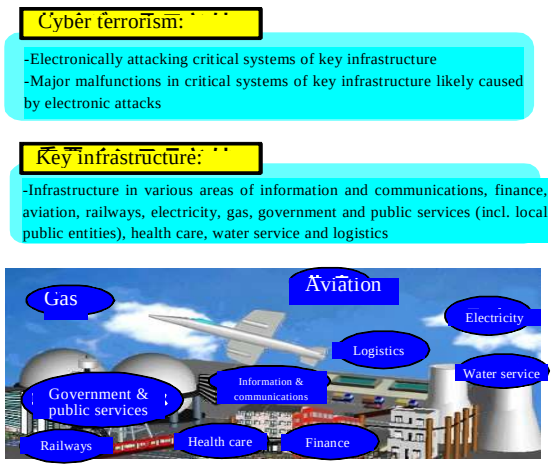
6. Measures Against Cyber Terrorism

(1) State of Cyber Terrorism

Communication and information networks are highly developed in modern society. If a cyber-attack were to strike critical systems in such key infrastructure, it could severely disrupt people's lives and socio-economic activity.

Cyber attacks can hit at any time or place if the attacker gains access to the computer or network. That being the case, cyber terrorism has become more and more of a real threat, as illustrated with the following examples.

Figure 15: Cyber terrorism and key infrastructure



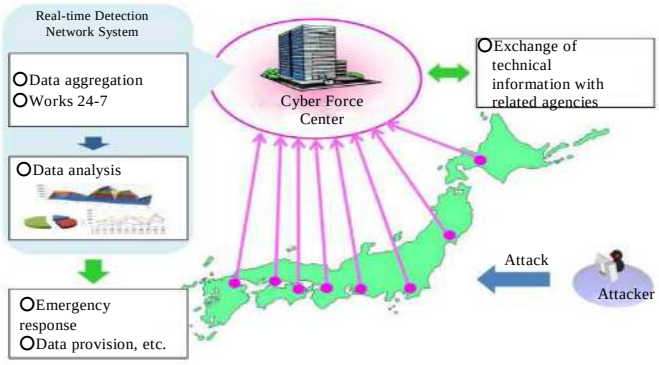
Case: In September 2010, a Chinese hacker group known as the Honker Union called for cyber attacks on Japanese government agencies on the website of a private organization claiming Chinese ownership of the Senkaku Islands. There was then a large concentration of site accesses on the NPA website that appeared to be related to this, overloading the server and making the site hard to view.

(2) Structure to Combat Cyber Terrorism

Cyber Terrorism Countermeasure Promotion Office has been established at the NPA. This office guides and coordinates anti-cyber terrorism measures for prefectural police, and promotes comprehensive anti-cyber terrorism measures, such as training for prefectural police personnel.

In addition, technical forces referred to as Cyber Forces have been established in each Regional Police Bureau as the technical underpinnings of anti-cyber terrorism measures. The Cyber Force Center, residing at NPA, acts as the control tower for the Cyber Forces nationwide. The center works around the clock to detect signs of cyber terrorism, also providing valuable services to key infrastructural companies by analyzing aggregated data and providing results to such companies.

Figure 16: Function of the Cyber Force Center



(3) Anti-Cyber terrorism Initiatives

1) Promotion of Public-Private Partnership Against Cyber Terrorism

Police have a number of initiatives for preventing cyber terrorism and accurately responding when attacks do occur. Besides providing key infrastructural companies and other companies with information on separate cyber terrorist threats and information security, the police run joint training with these companies for expected forms of cyber terrorism and promote anti-cyber terrorist measures with public-private partnerships to help improve emergency response capabilities.

2) Strengthening International Ties

Cyber terrorism crosses international borders with ease and is not a problem that can be solved by any one country alone. As such, police work hand-in-hand with related foreign institutions and organizations to regularly exchange information that may help in the fight against cyber terrorism and take measures such as holding joint training exercises in order to respond appropriately in case of incidents.

Section 3: Sweeping Enhancement of Anti-Cybercrime Measures

1. Enhancing Measures Against Unauthorized Access

(1) Study for Strengthening Enforcement

Current Unauthorized Computer Access Act is limited in that arrest is only permitted if someone succeeds in actually gaining unauthorized access. Police therefore need to study measures to prevent damage that may occur at the various stages which lead to unauthorized access.

(2) Improving Access Administrator Prevention Measures

A framework to promote and support access control functions needs to be reviewed as the basis for voluntary advancement initiatives by private companies.

2. Improving the Environment for Cybercrime Investigations

(1) Measures to Enable Identification of Internet Café Users

Enabling identification of internet cafe users is essential to deter crimes originating in cafes. Since 2007, the NPA has proposed several measures to the Japan Complex Cafe Association to confirm the identity of cafe users and eliminate their anonymity.

Prefectural police have also established internet cafe liaison councils. These councils exchange information with internet cafe operators and allow the police to

propose various measures to all operators to eliminate anonymity of cafe users, such as confirmation of user identity, recording terminals used, and installation of security cameras.

(2) Measures to Prevent Abuse of Wireless Networks and Mobile Data Cards

People connecting to the Internet with another name by accessing other people's wireless network without authorization presents the possibility for security issues. An appeal needs to be made to manufacturers and distributors about wireless network equipment being sold with default encryption settings.

With regards to mobile data cards, the problem lies with users being able to anonymously purchase cards without their identity being confirmed. An appeal needs to be made to businesses to confirm identity at time of purchase, and the businesses need to spur on such initiatives voluntarily.

(3) Saving Communication Logs

In cybercrime investigations, detectives must identify both what computer was used and who was using that computer. Police need to deepen public understanding of the importance of communication logs in making such identification.

3. Maintaining Cyberspace Order Through Public-Private Partnerships

Police need to bring public and private parties together and continue initiatives to maintain order in cyberspace by supporting initiatives run by private groups in terms of cybercrime volunteer activity, blocking child pornography, and preventing the victimization of children on social networking sites.