DOI 10.15302/J-SSCAE-2016.06.019

Trends in and Management of Bad Cyberspace Information Around the World

Jia Yan[1], Li Aiping[1], Li Yuxiao[2], Li Shudong[1], Tian Zhihong[3], Han Yi[1], Shi Jinqiao[4], Lin Bin[1]

1. Computer School of National University of Defense Technology, Changsha 410073, China
2. Chinese Academy of Cyberspace Studies, Beijing 100010, China
3. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, Sichuan, China
4. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: In view of the need to manage all kinds of bad information (including information pertaining to terrorism, rumors, fraud, violence, pornography, and subversion) in cyberspace, this paper summarizes the management of bad cyberspace information around the world. This paper first introduces the definition and classifies bad information, proposes laws and regulations for bad information supervision, and expounds on what countries legislate. Second, starting with network data monitoring, information filtering, and the confrontation of public opinion, this paper introduces the techniques and means of Internet governance pertaining to bad information. Finally, this paper describes recent global internal Internet governance special actions.
Keywords: cyberspace; bad information; information supervision; information filtering; public opinion confrontation

1 Introduction

There are multiple factors in the production and propagation of bad cyberspace information. First, understanding and regulating bad information are two different areas of endeavor. There are issues such as lack of boundaries, openness, and multiple accesses that lead to the proliferation of bad information. Secondly, the younger age of netizens and differences in netizen quality have increased the number of subjects who produce and spread bad information. Finally, we have expanded from the physical world to cyber space. Controlling the production and propagation of bad cyber information and making it no longer harmful to society has become an important global objective. Recently, most countries have adopted legislative supervision, special action, and comprehensive management mode of various technical means in the supervision of bad information, and have achieved favorable results.

2 Definition and classification of bad information

The national conditions and legal systems of the world are not the same, so there are differences in the definitions pertaining to bad information on the Internet. Some countries or international organizations use "Internet bad information," "Internet illegal information," "Internet unhealthy information," "Internet spam," and "Internet unfair and harmful information" to refer to the relevant information. Although the appellations are not the same, the commonality is that bad information poses a threat or damages national security, social order, and individual interests.

We defined "bad cyberspace information" as spreading information violating the constitution and provision of laws and regulations, contrary to the public interest or morals, or harmful to the state, society, or personal interests. Bad Internet information has two characteristics: First, it exists in digital form and spreads on the Internet; second, it is harmful. This information includes

Received date: 12 October 2016; **revised date:** 20 October 2016
Corresponding author: Jia Yan, Computer School of National University of Defense Technology, Professor. Major research field is network and information security, and online social network analysis. E-mail: apli1974@gmail.com.
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10).
Chinese version: Strategic Study of CAE 2016, 18 (6): 094–098
Cited item: Jia Yan et al. Trends in and Management of Bad Cyberspace Information Around the World. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.019

video, audio, pictures, text, computer programs, and other forms that endanger national security, damage racial or national unity and dignity, destroy state power, further terrorist activities, endanger social order, spread pornographic content, promote cults and superstitions, defraud public and private property, infringe on privacy and reputation, and other aspects of content.

The United States divides the bad Internet information into the following types: ① spreading political incitement, terrorism, provoking ethnic conflicts or ethnic hatred and racial discrimination, and other information damaging national security and national dignity; ② spreading obscenity and pornography; ③ abuse of marketing information pertaining to minors; ④ infringing citizens' privacy, reputation, and portraiture right, including the spread of private information about others, or maliciously vilifying others; ⑤ violent information, including Internet slander and personal attacks; and ⑥ fraudulent information, including that pertaining to online gambling [1].

The UK divides bad Internet information into three categories: ① illegal information endangering state security and other prohibited rules under national law, such as child pornography, online fraud, etc.; ② bad information including the incitement of religious or racial hatred, or encouraging or abetting suicide; and ③ nasty information such as that pertaining to violence [2].

Germany mainly divides bad Internet information into Nazi extremist ideology, racism, violent information, online fraud, and child pornography [3].

By combining the major countries' definitions of bad information, integrating the common parts and their respective foci, this paper divides bad Internet information into the following six categories: ① endangering state security and national dignity; ② Internet pornography and violence; ③ cults and superstition; ④ rumors and slander; ⑤ fraud and illegal transactions; and ⑥ invasion of privacy and personal rights and interests.

3 Regulatory laws on bad Internet information in various countries

3.1 Endangering national security and national dignity

The United States has successfully enacted the Economic Espionage Act to regulate information that may endanger government interests. The aim of the Homeland Security Bill and the Patriot Act is to manage sensitive information and prevent terrorism. The Hate Crimes Prevention Act of 2009 limited the scope of inciting hate regarding race, color of skin, religion, gender, sexual orientation, or disability, especially for those people who make violent attacks based on sexual orientation, gender, or disability. Such behavior is regarded as a crime, and in some cases, those people can be sentenced to death.

On January 23, 2003, the European Union passed the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems. This protocol regulates information about racism and xenophobia as the main members, France and Britain, introduced an anti-terrorism bill to regulate information regarding terrorism.

To prevent the spread of terrorism through the Internet, Russia issued the WiFi Real-Name Certification, the New Rules of Prominent Bloggers, and the Mass Media Act; Australia promulgated the Classification (Publications, Films, and Computer Games) Act 1995. To regulate information that endangers national security and national interests, Korea introduced the Act on Promotion of Information and Communications Network Utilization and Data Protection; and Singapore promulgated the Internet Code of Practice, supplemented by the Sedition Act to regulate information inciting ethnic hatred.

3.2 Internet pornography and violence

To protect teenagers, many countries introduced related measures and legislation. In terms of the overall regulation of information harmful to teenagers, the UK Council for Child Internet Safety (UKCCIS)'s Advice on Child Internet Safety 1.0; Singapore's Law of the Network Behavior and Operation Procedures of the Internet; South Korea's Act on Promotion of Information and Communications Network Utilization and Data Protection; and Japan's Assure the Safety of Surfing on the Internet for Teenagers are clear about the scope of bad information. In terms of regulation, Germany's Youth Protection Act in Public Places and Guidelines issued by the Land Media Institutes on ensuring protection for young persons (youth guidelines) and Russia's Law on Protecting Children from Negative and Harmful Information limit the interference of bad information.

To regulate child pornography, the Children's Internet Protection Act was introduced in the United States. The UK enacted the Memorandum of Understanding: Sexual Offences Act 2003 and the Safety Net Agreement regarding Rating, Reporting and Responsibility, the European Union introduced Electronic Europe, and France promulgated the Minors Protection Act. For further restrictions on minors' access to pornographic information, the United States introduced the Protection Act, supplemented by a content grading system. South Korea and Australia also use a grading system. Germany introduced the Block Landing Page Act to block web pages related to child pornography.

3.3 Internet fraud and illegal trade

In 1986, the United States took the lead in introducing the Computer Fraud and Abuse Act, the Secret Service was given the power to investigate Internet crimes, and rules were established protecting citizen's private property on the Internet. After many revisions, this Act was integrated into the United States Code. The Act provides a guiding role for other countries to formulate relevant laws and regulations.

In 2000, Russia supplemented content about illegal trading on the Internet in the Mass Media Act. In 2001, Australia promulgated the Interactive Gambling Act to ban Internet gambling, and the Fraud Act 2006 in the UK changed the definition of fraud. All in all, Internet law shows that the Internet's influence on economics is becoming greater, and governments are paying more attention to controlling the Internet.

In addition, in view of Internet rumors and slanders, invasion of privacy and personal rights, spam, and so forth, countries use various relevant laws and regulations to manage these concerns.

4 Internet governance techniques and means in various countries

According to the discovery, disposal, and the forensic process, bad Internet information management techniques mainly fall into three categories: Internet data monitoring, harmful information filtering, and public opinion confrontation.

4.1 Internet data monitoring system

After the 9/11 terrorist attacks, the United States government secretly launched a massive intelligence-gathering program. National Security Agency monitoring programs include the Prism Program, which was revealed by Edward Snowden. Other plans include Upstream, Fairview, Unbounded People, and Xkeyscore. The Upstream Project is one of the United States intelligence agencies' external monitoring programs, and, as an Upstream plan, the Upstream Project collects data such as submarine cables. In addition, the FBI's monitoring projects include MainCore, DCSNet, Slides, and so forth.

The Temporal Project was an intelligence surveillance project carried out by the UK Government Communications Headquarters (GCHQ) in early 2012. An interceptor was installed at the British landing of the transatlantic cable from North America with the main purpose of obtaining international telephone and network information, data transfers, and analysis.

Frenchelon is the "French Echelon," a project of intelligence gathering and network analysis operated by the French Directorate of the External Security. It has existed since the fall of the Berlin Wall in the early 1990s, with the aim of monitoring telephone calls, mail, and facsimiles. It also deciphers and interprets satellite passwords and so forth.

4.2 Harmful information filtering system

Net Nanny [4] is content filtering software developed by ContentWatch Holdings, Inc. in the United States in 1995. The purpose is to filter out all the bad information on the Internet to ensure that Internet users have access to safe web pages. Cyber Patrol [5] was developed by America's SurfControl Company in 1995 as a parental control and enterprise Internet access control software system.

The Internet Chat Dictionary [6] was developed by UK In Loco Parentis Company, to help parents decipher the abbreviations and passwords used by their children in Internet chat rooms to prevent them from falling into Internet porn traps. Anti-Porn parental controls [7], developed by Tueagles Company, are designed specifically for minors to protect children and avoid their exposure to with pornographic web pages.

The Wedge Web Filter App [8] is web filtering software developed by Webroot, a company in Canada. The software uses the web categorization database to provide the most comprehensive categories, and can improve the accuracy of the classification through manual auditing. I-FILTER Commercial Edition is a server-based web filtering software developed by a Japanese information security company Digital Arts.

4.3 Public opinion confrontation

Operation Earnest Voice is run by the United States Central Command, and was started in 2010. The purpose of the operation is to combat al-Qaeda supporters on the Internet and other organizations that have fought United States-led coalition forces.

On February 25, 2014, the "Russia Today" television website ran a story on Prism Door, which was exposed by Edward Snowden via a document showing that the project was run by the United States, Britain, Canada, Australia, and New Zealand. These five countries' spy agencies formed a "five-eye" spy alliance responsible for this spy project. The goal of the project was to disseminate false information on the Internet to manipulate web-based speech, thereby altering the information available to the Internet users and getting the results that government agencies want.

The Joint Threat Research Intelligence Group is a secret spy agency of the GCHQ, the UK intelligence agency. The group is responsible for destroying, smearing, and dividing the enemy, including Iranians, the hacker organization "Anonymous," and so forth. The agency has developed a variety of tools to manipulate online public opinion, including manipulating online survey results, creating false traffic, and filtering "extreme" information.

5 Special action on global bad Internet information management

5.1 Special action on Internet obscenity and pornography management

In 1995, the Federal Bureau of Investigation (FBI) launched a special initiative called the Innocent Images National Initiative. The action is an information driven initiative using active and multi-sectoral cooperation with the aim of combating Internet child pornography and associated crimes.

In May 2002, the UK launched a special action called Operation Ore, which targeted 7 272 British people who used the Landslide Productions Company website managed by the FBI

for the use of child pornography services; the agency launched an investigation and prosecuted them.

In January 2003, the media exposed a Canadian special investigation into child pornography called Operation Snowball. This action launched an investigation into 2 329 Canadian users exposed by America's Operation Avalanche who used the Landslide Productions Company website to obtain child pornography.

5.2 Special action on Internet extreme terrorism management

In June 2011, the European Union began a project to reduce illegal information and filter data on the Internet, especially violent terrorist content. The project was known as the Clean IT Project. Its main purpose is to form a consensus document and drive the Internet to help the government find information that incites violence and terror in the form of videos, images, text, and so forth.

In January 2014, the European Commission adopted action plans for the prevention of extreme and violent behavior and promoted them to member states. The plans summarized information against violent extremism, and member states were required to strengthen relevant measures to prevent extremist behavior that could lead to violence.

In February 2015, the White House announced close cooperation with technology companies against al-Qaeda and Islamic countries' special operations regarding network activity, and promoted the plan to cater to organizations that publish information on the Internet.

5.3 Special action on Internet rumors and slanders management

In 2008, the Korean government began to regulate bad information on the Internet, including managing online rumors and slanders. The action was carried out by police in South Korea, who regularly targeted rumors and malicious replies regularly to centralized management, arresting publishers who replied maliciously.

In April 2011, in view of the Japanese earthquake, Internet rumors appeared online regarding earthquakes and nuclear radiation. Japan's Ministry of Internal Affairs and Communications issued a notice requiring the telecommunications industry associations to take appropriate special measures to eliminate harmful rumors while protecting free speech.

On May 3, 2015, the Singapore Media Administration (MDA) closed The Real Singapore website operated by Ai Takagi and Yang Kaiheng as well as its Facebook, Twitter, and other social media and mobile applications.

6 Conclusions

With the rapid growth of information on the Internet, network access methods are increasingly diverse, and avoiding the pollution of harmful information is an urgent problem. Harmful, bad information has an impact on people's physical and mental health as well as a major impact on social stability, national unity, and even national security. This paper summarizes the current situation and trends in the management of bad information in cyberspace through describing the laws and regulations, technical means, and special actions of major countries around the world.

References

[1] Wang J. Research on legal issues of network communication [M]. Beijing: Mass Press, 2006. Chinese.

[2] Dong N. Cyber War [M]. Beijing: China Press, 2009. Chinese.

[3] Zheng Q H. Internet supervision in German must be laws to go by [EB/OL]. (2010-02-01) [2015-05-18]. http://news.xinhuanet.com/world/2010-02/01/content_12912508.htm. Chinese.

[4] Net Nanny [EB/OL]. (2015-05-18) [2016-08-15]. http://www.netnanny.com/.

[5] Cyber Patrol [EB/OL]. (2015-05-18) [2016-08-15]. http://www.cyberpatrol.com/.

[6] In Loco Parentis anti-grooming software [EB/OL]. (2015-05-18) [2016-08-15]. https://technologyinside.com/2007/02/07/in-loco-parentis-anti-grooming-software/.

[7] Anti-Porn parental controls [EB/OL]. (2015-05-18) [2016-08-15]. http://www.parental-controls.net/.

[8] Wedge web filter network app: Monitor, filter, and report on web usage at the network [EB/OL]. (2015-05-18) [2016-08-15]. http://www.wedgenetworks.com/lit/WedgeWebFilter-15082014.pdf.