

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Greenbelt Division**

**Du Daobin, Zhou Yuanzhi, Liu Xianbin, :
and Does 1-10, :**

Plaintiffs :

v. :

CISCO Systems, Inc. :
170 West Tasman Drive :
San Jose, CA 95134 :

Thomas Lam :
President of China Operations :
CISCO Systems, Inc. :
170 West Tasman Drive :
San Jose, CA 95134 :

Owen Chan :
President of Asia Pacific Operations :
CISCO Systems, Inc. :
170 West Tasman Drive :
San Jose, CA 95134 :

Rick Justice :
Executive Advisor :
Office of the Chairman and CEO :
CISCO Systems, Inc. :
170 West Tasman Drive :
San Jose, CA 95134 :

John T. Chambers :
Chairman and CEO :
CISCO Systems, Inc. :
170 West Tasman Drive :
San Jose, CA 95134 :
Defendants. :

COMPLAINT

Plaintiffs, by and through their attorneys, allege upon personal knowledge and belief as to their own circumstances, and upon information and belief (based on the investigation of counsel) as to all other matters, that substantial evidentiary support exists or will exist after a reasonable opportunity for further investigation and discovery as a result of trial proceedings, in support of the following:

1. Named Plaintiffs and additional unnamed and to be identified Plaintiffs (hereinafter referred to collectively as “Plaintiffs”) have been and are being subjected to grave violations of some of the most universally recognized standards of international law, including prohibitions against torture, cruel, inhuman, or other degrading treatment or punishment, arbitrary arrest and prolonged detention, and forced labor, for exercising their rights of freedom of speech, association, and assembly, at the hands of Defendants through Chinese officials acting under color of law in the People’s Republic of China (referred to herein as “the PRC” or “China”).

2. To commit these violations of specific, universal, and obligatory standards of international law, Defendants willingly and knowingly provided Chinese officials with technology and training to access private internet communications, identify anonymous web log (“blog”) authors, prevent the broadcast and dissemination of peaceful speech, and otherwise aid and abet in the violation of Plaintiffs’ fundamental human rights.

3. Defendants committed these acts knowingly and with actual knowledge of the consequences of their profit-seeking actions. Defendants’ own written and spoken statements make clear that Defendants sought to profit from PRC’s “Golden Shield” project as much as possible, and Defendants, while fully cognizant of the grave violations of universally recognized

standards of international law that would result from the “Golden Shield” project, chose to aid and abet PRC in its efforts to create, maintain, and expand the Golden Shield and did indeed profit substantially as a result.

4. Defendants’ knowing and willful actions, in providing substantial aid, assistance, and encouragement to the PRC in the creation, maintenance and expansion of the Golden Shield, served and are continuing to serve as the basis for the acts of persecution and torture that occurred and are occurring as a direct result of Defendants’ activities. In so acting, Defendants knowingly and willfully aided and abetted in the commission of torture, cruel, inhuman, or other degrading treatment or punishment, arbitrary arrest and prolonged detention, forced labor and other major abuses violating international law that caused Plaintiffs severe physical and mental pain and suffering.

5. Plaintiffs’ claims are actionable under the Alien Tort Statute (ATS), 28 U.S.C. § 1350, and the Torture Victim Protection Act (TVPA), 28 U.S.C. § 1350, because their injuries resulted from violations of specific, universal, and obligatory standards of international law as embodied in a number of treaty obligations binding on the United States and implemented domestically here in the United States by a number of statutes including the TVPA.

6. Defendants’ conduct also violates Maryland state laws, including prohibitions against battery, false imprisonment, assault, intentional infliction of emotional distress, and/or negligence.

7. Defendants’ conduct also breaches United States law under the Electronic Communications Privacy Act by exceeding their authorization to access and control highly private and potentially damaging information concerning Plaintiffs’ electronic communications, in violation of 18 U.S.C. § 2701, by unlawfully and knowingly divulging Plaintiffs’ electronic

communication contents and user information, in violation of 18 U.S.C. § 2702, and by intentionally acquiring and/or intercepting the contents of electronic communications sent by and/or received by Plaintiffs through their use of computers, routing equipment and other electronic devices which were part of, and utilized in, Defendants' electronic communications systems, in violation of 18 U.S.C. § 2511.

8. Defendants' conduct also breaches United States law in that Defendants' actions are in direct violation of the "Tiananmen Square sanctions"¹ which included a suspension of export licenses for crime control and detection instruments and equipment.

9. Plaintiffs seek general, compensatory, and punitive damages for their injuries, as well as declaratory and injunctive relief to hold Defendants accountable for their unlawful actions, and to secure Defendants' assistance in obtaining the Plaintiffs' release from prison. Plaintiffs also seek relief that would prevent Defendants from similarly harming others in the future.

JURISDICTION AND VENUE

10. This Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1331 (federal question jurisdiction), 28 U.S.C. § 1350 (Alien Tort Statute), 28 U.S.C. § 1350 (Torture Victim Protection Act) and 18 U.S.C. § 2701 *et seq.* (The Electronic Communications Privacy Act). The Alien Tort Statute provides federal jurisdiction for "any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States." The Torture Victim Protection Act supplements and confirms the ATS by providing federal court jurisdiction for acts of torture, as defined by 28 U.S.C. § 1350. The Electronic Communications Privacy Act, 18

¹ See Sec. 902 of the Foreign Relations Authorization Act, Fiscal Years 1990 and 1991 (P.L. 101-246; 22 U.S.C. 2151 note).

U.S.C. § 2701 *et seq.*, provides federal jurisdiction for civil claims arising from unauthorized disclosure of electronic communications and customer information.

11. This Court also has supplemental jurisdiction over claims arising from violations of state law because, pursuant to 28 U.S.C. § 1367, the facts in the claims arising from state law are so related to the Plaintiffs' claims under federal laws that they form part of the same case or controversy under Article III of the United States Constitution.

12. Venue in this District is proper because Defendant CISCO Systems, Inc. ("CISCO") maintains a permanent office in this District, does business in this District, and has substantial and ongoing business contacts in this District, including with certain Federal Government clients that are located in this District. The individual (non-corporate) Defendants are similarly subject to the jurisdiction of this court by virtue of their corporate ties with CISCO and/or business contacts and activities in this jurisdiction.

PARTIES

Plaintiffs

13. Plaintiff **Du Daobin** ("Du") is a subject, citizen, and resident of the People's Republic of China. He sues on behalf of himself for the injuries, including severe pain and suffering, he has endured as a result of his torture, cruel, inhuman, or other degrading treatment, and arbitrary arrest and prolonged detention inflicted upon him as a result of Defendants' actions aiding and abetting Chinese government officials in committing these major human rights abuses. Specifically, **Du Daobin** was arrested, unlawfully detained, and prosecuted for publishing and circulating internet articles calling for fair treatment of rural farmers in addition to strong criticisms of the Chinese Communist Party ("CCP"). He also sues for compensation for property seized by government officials in conjunction with his unlawful and prolonged

detention. Previously a victim to unlawful detention, torture, and house arrest, Du remains closely monitored and restricted to Yingcheng City. As a result of Du's harassment, his wife has moved out and left him to raise their child.

14. Plaintiff **Zhou Yuanzhi** ("Zhou") is a subject, citizen, and resident of the People's Republic of China. He sues on behalf of himself for the injuries, including severe pain and suffering, he has endured as a result of his torture, cruel, inhuman, or other degrading treatment, and arbitrary arrest and prolonged detention inflicted upon him as a result of Defendants' actions aiding and abetting Chinese government officials in committing these major human rights abuses. Specifically, **Zhou Yuanzhi** was arrested, unlawfully detained, and prosecuted for publishing and circulating internet articles that support human rights and democratic reform in China, as well as serving as a reporter for the Laogai Research Foundation ("LRF"). He also sues for compensation for property seized by government officials in conjunction with his unlawful and prolonged detention. Previously a victim to unlawful detention, torture, and house arrest, Zhou is currently a prisoner in his own home while his family bears the significant consequences of his political discrimination.

15. Plaintiff **Liu Xianbin** ("Liu") is a subject, citizen, and resident of the People's Republic of China. His wife Chen Ming Xian so authorized this suit on behalf of her husband, Liu Xianbin, for the injuries, including severe pain and suffering, he has endured as a result of his torture, cruel, inhuman, or other degrading treatment, and arbitrary arrest and prolonged detention inflicted upon him as a result of Defendants' actions aiding and abetting Chinese government officials in committing these major human rights abuses. Specifically, **Liu Xianbin** was arrested, unlawfully detained, and prosecuted for publishing and circulating internet articles that support human rights and democratic reform in China, as well as communicating with other

Chinese reform advocates. He also sues for compensation for property seized by government officials in conjunction with his unlawful and prolonged detention. He is currently serving a ten-year sentence in the Chuanzhong Prison. He was sentenced on March 25, 2011 for “inciting subversion of state power.” He has currently served over two months of his ten-year sentence.

16. Additional Plaintiffs temporarily designated as “**Does 1-10**” are citizens of China currently living in China or in exile in other countries, such as the United States, who were arbitrarily detained, arrested, tortured, subjected to cruel, inhuman, or degrading treatment or punishment, and/or subjected to forced labor, as a result of Defendants’ actions in aiding and abetting these violations of United States and international law, including federal and state laws that provide civil actions for Defendants’ acts. At the time of filing, Plaintiffs have identified hundreds of individuals arbitrarily imprisoned in China for expressing their support for free elections, democracy, or human rights through internet communications or use and whose arrests and detention are directly linked to Defendants’ knowingly aiding and abetting the PRC’s unlawful acts. Additional information about their arrests and detention, and their treatment in detention, for these unnamed individuals, as well as information about how Defendants may be responsible for their abuse, will be obtained during discovery and described in greater detail during these proceedings. Their inclusion in this lawsuit is critical both in order to identify the extent of Defendants’ role in enabling these abuses, as well as to curb, prevent and remedy current corporate practices of Defendants that are directly responsible for these abuses. Such Plaintiffs may also include others located outside of China who have been or are currently being adversely affected by Defendants’ practices.

Defendants

17. Defendant **CISCO Systems, Inc.** (“CISCO”) is a California Corporation with offices and locations worldwide. CISCO is one of the world’s largest technology corporations. CISCO is headquartered in San Jose, California, and has offices and a substantial and ongoing business presence in this District. CISCO designs and sells networking, voice, and communications technology and services. In doing so, CISCO facilitates the distribution of and access to electronic communication and information through internet networking technology including CISCO Internet Protocol-based networking solutions.

18. Defendant Thomas Lam has served as the President of CISCO’s China Operations since 2005. In this capacity, Mr. Lam oversees CISCO’s service and support operations to the PRC. In December 2006, Mr. Lam was selected as “IT Figure of the Year” by China Computer World. Additionally, Mr. Lam has served as the Vice Chairman of CISCO Greater China since January 2010 where he is responsible for developing and driving strategies for corporate social responsibility, corporate affairs and university relations in Greater China. In these capacities, Mr. Lam oversaw the sale of security technology products and services used by the PRC.

19. Defendant Owen Chan served as Senior Vice President, Asia Pacific Operations at CISCO from August 2005 to February 2010. Originally joining CISCO in 1999, Mr. Chan has been the President and CEO of the Greater China Theater at CISCO since February 2010. As President and CEO of the Greater China Theater, Mr. Chan is responsible for developing and executing a strategy for marketing CISCO’s goods and services to clients in China.

20. Defendant Rick Justice served as the Executive Vice President of Worldwide Operations and Business Development until his retirement in 2009. In this capacity he oversaw the organization’s thousands of sales, systems engineering, and operations employees. Joining

CISCO in December 1996, Mr. Justice was a key proponent in evolving CISCO's strategy to capture opportunities in emerging markets like China, which helped CISCO double its business in emerging markets in over a three year period. Mr. Justice currently serves as Executive Advisor to the Office of Chairman and CEO.

21. Defendant John Chambers is the Chairman and CEO of CISCO. Mr. Chambers joined CISCO in 1991 as Senior Vice President, Worldwide Sales and Operations. He has served as CEO since 1995, where he has overseen CISCO's dramatic growth from a corporation with \$1.2 billion in annual revenue in 1995 to roughly \$40 billion in annual revenue in recent times. Mr. Chambers has overseen all of the organization's operations, including the design, marketing, and sale of services and communications technology in China.

STATEMENT OF FACTS

General Facts

22. China has the world's largest population of internet users. China currently has a population of 1.34 billion with approximately 457 million being internet users. Such expansive access to the internet in China has the potential to provide the Chinese people with unparalleled access to information in addition to a venue for public expression and open dialogue on important civic issues.

23. As early as 1998, the CCP sought to prevent the Chinese people from the free expression of their views by aggressively monitoring the internet, intimidating Chinese internet users, and preventing the dissemination of "harmful" internet content. The Chinese government places strict controls on politically sensitive internet content such as human rights issues in China, the Tiananmen Square massacre, democratic reform in China, and all opposition to the CCP.

24. The CCP's internet censorship began with the creation of a nationwide surveillance program called the Golden Shield Project, which was launched by China's Public Security Ministry no later than November 2000. The Golden Shield Project, also known as the "Great Firewall of China," is a sophisticated system of internet filters and censoring techniques which restricts access to a variety of content disfavored by the CCP. The Golden Shield Project is officially justified as a method to enhance the ability of the CCP to combat criminal activity, but, in reality, it is widely used to suppress peaceful political, social, and religious dialogue of dissent.

25. The CCP employs a substantial number of internet police to implement the Golden Shield Project, who assist the CCP in preventing the Chinese people from the free expression of their views on the Internet. The CCP employs what has been estimated as between at least 30,000-50,000 internet police. These internet police further the objectives of the CCP by monitoring, tracking and shutting down Internet Protocol (IP) addresses, monitoring, tracking and shutting down e-mail addresses, censoring internet browser search results, and censoring other material the CCP opposes.

26. The Golden Shield Project has recently curtailed Chinese internet user freedom by blocking content as common as global current events. Earlier this year, the CCP, utilizing the Golden Shield, heavily censored the pro-democracy revolutions in North Africa, especially in Tunisia and Egypt. On or about January 28, 2011, the CCP began censoring internet content associated with the search term "Egypt." The CCP censorship started only three days after the Egyptian uprising began.

27. In addition, the Golden Shield Project has blocked or censored nearly all internet content that mentions Liu Xiaobo, the 2010 Nobel Peace Prize laureate. The Golden Shield

Project's enhanced police state capabilities were used against Mr. Liu. In 2009, Mr. Liu was prosecuted for "inciting subversion of state power" and sentenced to eleven years of prison for urging the Chinese government to move towards a freer, more democratic society in his online writings.

28. CISCO aggressively sought contracts to provide substantial assistance in helping the Chinese government implement the Golden Shield Project. In a 2002 presentation, CISCO described the Golden Shield Project as a source for CISCO opportunities in the areas of planning, construction, technical training, and maintenance. See Exhibit A, CISCO publication titled "Overview of the Public Sector."

29. In that 2002 CISCO publication, CISCO proffered that networking services were a future direction for security products, showing that CISCO recognized opportunities for future business with the Chinese government.

30. In that 2002 CISCO publication, CISCO recognized that its services and products would be utilized, *inter alia*, by law enforcement, prisons, forced labor camps, and "forced custody and repatriation centers." See Exhibit A, p. 9. Such uses are in direct violation of the "Tiananmen Square Sanctions."

31. In that 2002 CISCO publication, CISCO recognized that its services and products would be utilized, *inter alia*, by CCP's "internet police" and CCP's "information and communication police." See Exhibit A, p. 12 & 14.

32. In that 2002 CISCO publication, CISCO recognized that its services and products would be utilized by CCP for, *inter alia*, "Internet monitoring & supervision." See Exhibit A, p. 19.

33. In that 2002 CISCO publication, CISCO recognized that its services and products would be utilized by CCP to, *inter alia*, “Drive high-level planning and high standard construction of ‘The Golden Shield Project.’” See Exhibit A, p. 49.

34. In that 2002 CISCO publication, CISCO recognized that “Digitalization and networking represent [the] future direction of security protection products.” See Exhibit A, p. 50.

35. In that 2002 CISCO publication, CISCO recognized that one of the purposes of the Golden Shield Project (which CISCO was marketing itself to be a part of) was to “Stop the network-related crimes.” See Exhibit A, p. 57.

36. In that 2002 CISCO publication, CISCO recognized that one of the purposes of the Golden Shield Project (which CISCO was marketing itself to be a part of) was to “Guarantee the security and services of [the] public network.” See Exhibit A, p. 57.

37. In that 2002 CISCO publication, CISCO recognized that one of the purposes of the Golden Shield Project (which CISCO was marketing itself to be a part of) was to “Combat ‘Falun Gong’ evil religion and other hostiles.” See Exhibit A, p. 57.

38. In that 2002 CISCO publication, CISCO recognized that its services and products would be utilized by CCP to, *inter alia*, help “Gain police strength from science & technology” and that CISCO’s products would/could be utilized for the creation of a “Prevention & control system of public security.” See Exhibit A, p. 62-63.

39. In that 2002 CISCO publication, CISCO marketed itself as a provider of “E-learning” to CCP. See Exhibit A, p. 70.

40. As a result of these and other marketing efforts by CISCO, CCP chose to work with CISCO and CISCO successfully aided CCP in the implementation of CCP's Golden Shield Project.

41. In 2004, Zhang Sihua, the vice president for a Chinese branch company of CISCO said that CISCO was "very glad to cooperate with the police department in building up the first level network of the Golden Shield." It was additionally reported that in 2004, through the use of CISCO routers and other related products, CISCO helped construct the first level network of the Golden Shield Project.

42. In materials submitted to the House of Representatives Committee on International Relations during a 2006 hearing of the 109th United States Congress, the following facts were disclosed:

a. CISCO has profited greatly by providing the Chinese government with the technology necessary to filter internet content through its creation of Policenet, one of the tools the regime uses to control the internet. CISCO's estimated profit from sales to China according to Derek Bambauer of *Legal Affairs* is estimated to be \$500 million and holds 60 percent of the Chinese market for routers, switches, and other sophisticated networking gear. The company anticipates that China will soon become its third largest market, just behind the U.S. and Japan.

b. [As of 2006, CISCO was under contract to provide] China with its 12000 Series routers, which are equipped with filtering capability typically used to prevent Internet attacks, but can also be used by [CCP] authorities to block politically sensitive information, according to the Congressional Research Service.

43. CISCO collaborated with the CCP to design and develop the Golden Shield Project to incorporate advanced information and communication technologies into security enforcement with the primary goal of creating a comprehensive online surveillance system specifically geared to enable and facilitate the suppression of dissident activity in China.

44. Prior to the Golden Shield Project's development, the CCP was unable to tightly monitor and strictly control China's internet activity. With the assistance of CISCO, the CCP is now capable of detecting, identifying and tracking perceived threats to the CCP's power, and blocking "harmful" websites.

45. Upon information and belief, CISCO employees customized themselves or trained others to customize CISCO's standard products to meet the Golden Shield Project's unique and non-standard surveillance objectives.

46. In material submitted to the House of Representatives Committee on International Relations during a 2006 hearing of the 109th United States Congress, the following facts were disclosed:

a. According to Harry Wu, The Executive Director of the Laogai Research Foundation, CISCO Systems has marketed its Policenet equipment specifically designed to make it easier for the Chinese Police to carry out surveillance of electronic communications. CISCO is also suspected of giving Chinese engineers training in how to use its products to censor the internet. Policenet currently operates in all but one of China's provinces. Policenet connects officials of the Public Security Bureau—a national agency with local branches that handle security, immigration, "social order," and law enforcement- to each other and to electronic records that store a wealth of information on every citizen in China.

Along with Policenet, CISCO also produced the watchdog router that prevents internet users in China from gaining access to banned websites.

b. Reporters Without Borders said that CISCO Systems has sold China several thousand routers at more than 16,000 euros each for use in building the regime's surveillance infrastructure. This equipment that was programmed with the help of CISCO engineers allows the Chinese authorities to read data transmitted on the internet and to spot "subversive" key words. The police are able to identify who visits banned sites and who sends "dangerous" e-mail messages.

47. In 2002, CISCO explicitly recognized that China uses forced labor as a part of its law enforcement strategy. In 2002, CISCO also recognized that China employs forced custody stations, forced repatriation centers, and forced education centers. See Exhibit A.

48. In 2002, CISCO explicitly recognized that one of the Chinese government's goals for the Golden Shield Project was to target disfavored groups. In its own presentation documents, CISCO quoted Li Runsen, the Chinese government's information technology lead who stated bluntly that the Golden Shield would be used to "Combat 'Falun Gong' evil religion and other hostiles." See Exhibit A, p. 57.

49. Recognizing both the enforcement strategy and targets of the Golden Shield Project, CISCO marketed and sold its products to the Chinese Government. In 2006, CISCO's Rick Justice, then senior vice-president for worldwide operations, stated that "[w]e sell to police organizations in many countries." Then, Mr. Justice went on to say that "[w]e do business [in China] the way we do business anywhere."

50. CISCO marketed internet management systems that could identify dissident internet behavior to the Chinese government and relay that information to Chinese law enforcement authorities.

51. Plaintiff is informed and believes that CISCO was fully aware that the Golden Shield Project would be used to commit human rights violations and violations of international law.

Specific Facts

Du Daobin

52. Since 2001, Du Daobin (“Du”) has published articles on Chinese websites calling for fair treatment of city and rural dwellers, social security and fair wages to farmers, and abolishment of the discriminatory policies of usury towards farmers. He has published articles on foreign websites strongly criticizing the CCP’s policies, ideals, and one-party dictatorship. Additionally, Du has initiated and participated in many petition protest activities on the internet.

53. On October 28, 2003, Du was criminally detained and arrested while his house was raided by Chinese authorities.

54. On June 11, 2004, Du was charged with “inciting to subvert state power” and was sentenced to three years in prison. His sentence, however, was suspended for four years.

55. From 2004 to 2008, the Public Security Bureau (“PSB”) communicated with Du approximately twice a month. Du was not able to use his real name to publish articles domestically or internationally; he was not allowed to leave China and his guests were tightly regulated, questioned and placed under surveillance. On many occasions, the PSB threatened to hinder the educational advancement of Du’s child. Additionally, the PSB regularly intercepted Du’s mail and royalty checks.

56. On July 21, 2008, the PSB reinstated Du's suspended sentence and raided his home. During his time in prison, Du was subject to physical and psychological torture. Du was imprisoned under the most stringent controls. He was forced to sit on a low bench for two months which led to cardiac prolapse and difficulty walking. Due to malnutrition and potassium deficiency, he lost his ability to walk without the assistance of others. During recovery, he was dependent on a wheelchair. At the same time, Du's wife was continually harassed and abused; and their child was under constant surveillance at school.

57. Despite Du's prison release in 2010, he is still-bound. On the day of his release, he was escorted to the Yingcheng City police department. Du was told not to publish anything and to report any departure from Yingcheng City. He must also report to and participate in weekly community service.

58. Du has been unemployed for over five months. He does not have stable income, is not allowed to leave the city for work and he is prohibited from leaving China. He survives on the generosity and assistance of his friends. His internet activity is constantly monitored, which has slowed down his connection's speed so much that it sometimes takes an hour to load one page. Additionally, he is constantly redirected to other webpages and is otherwise restricted from using the internet.

59. Due to the CCP's harassment of Du, his wife has moved out and left him to raise their child.

Zhou Yuanzhi

60. With the rise of the internet, Zhou Yuanzhi ("Zhou") became an active cyber writer. Since the beginning of the 21st century, Zhou has used both his real name and a pen name to publish online articles critical of the CCP.

61. In or about 2004, Zhou became a regular writer for “Guancha” (www.observechina.net), which is currently run by the Laogai Research Foundation (“LRF”).

62. From 2004 to 2008, he contributed over 40 articles to Guancha, promoting human rights and democracy in China.

63. In 2007, Zhou became a reporter for Guancha, spending a significant amount of time investigating human rights cases in China.

64. In the less than two years since he became a reporter for Guancha, Zhou wrote and published approximately 10 reports under a pseudonym.

65. His articles and activities were closely tracked by local police who, on many occasions, invited him to “drink tea” with them and warned him to stop writing.

66. On May 3rd, 2008, the local police finally lost their patience when they found in Zhou’s email that he was writing a report about China’s Laogai products for the LRF. The Jingmen City Public Security Bureau in Hubei Province placed him and his wife, Zhang Zhongfeng into a detention center.

67. For security reasons, Zhou kept the unfinished report and many related pictures in the draft folder of his Google email account. All the files were copied and deleted by the police on the day Zhou was detained.

68. Police searched Zhou’s home and confiscated his computer, camera, bank documents and other property.

69. Zhou was severely tortured in the detention center until he confessed that he was writing a report for LRF.

70. His wife was released three days later, but was placed under house arrest. Zhou was detained for twelve days and was released on May 15, 2008.

71. Due to a lack of evidence and increasing pressure from international communities, the local police sent Zhou home, but he was put under house arrest for nearly six months, until November 3, 2008.

72. Although the house arrest formally ended on November 3, 2008, the local police managed to make his home a prison. During the past three years, Zhou has been under constant police surveillance. The police have discretely placed a dozen surveillance cameras around his house. The police randomly enter Zhou's house to check his computer.

73. A prisoner in his own home, Zhou has no way to look for a job. His entire family is sustained by his wife's meager salary.

74. Political disloyalty is still considered a major offense, so Zhou's son was denied the opportunity to have a decent job after graduating from college. The entire family has fallen victim to political discrimination.

Liu Xianbin

75. For participating in the 1989 Tiananmen Square protests and writing articles demanding political reform, Liu Xianbin ("Liu") was sentenced on December 28, 1992 to two-and-a-half-years in prison for "counterrevolutionary propaganda and incitement."

76. After his release, he engaged in organizing a branch of the China Democracy Party in Sichuan, and was sentenced to thirteen years on August 6, 1999, on charges of "subverting state power."

77. During his years of imprisonment, Liu was kept under "strict surveillance." This "strict surveillance" meant Liu was given harsher discipline, harder work, higher likelihood of mistreatment, and less communication and contact with other inmates.

78. Liu was released on November 6, 2008 from Chuandong Prison (Eastern Sichuan Prison) and placed under close surveillance by local police. Despite constant police harassment, Liu was active in writing and disseminating articles on the internet that promoted human rights and democratization in China. Many of his articles were published on overseas websites, including “Guancha” (www.observechina.net), run by the LRF.

79. Liu was under physical surveillance with police vans parked in his neighborhood constantly monitoring his words and actions. Liu’s house is constantly searched and his property is confiscated. Additionally, Liu’s activity on the internet is closely monitored. Police know of every article he has published and every message he has exchanged online.

80. Between 2009 and 2010, Liu was intimidated by police who threatened to send him back to prison unless he stopped writing. Liu did not comply because he believes freedom of speech is a basic human right.

81. On June 27, 2010, Liu was detained by police of Suining on suspicion of “inciting subversion of state power.” On July 21, 2010, the Suining PSB wrote a Recommendation Indictment to the Suining Procuratorate, requesting that Liu be indicted for “inciting subversion of state power” because he published and disseminated “subversive” articles online.

82. On the same day Liu was detained, the police ransacked his home and confiscated his computer, books and magazines, and various media storage devices. None of these items have been returned.

83. On March 25, 2011, Liu was sentenced to ten years in prison for “inciting subversion of state power.” Liu received this sentence because of articles that he published during April 2009 and February 2010 in overseas Chinese magazines and websites.

84. After the trial, Liu was put into Chuanzhong Prison (Central Sichuan Prison). Because he is a repeat offender and refused to confess his guilt, the prison officials and police treated him harshly. The first day he was in prison, he was assaulted by other prisoners at the encouragement of the prison police.

85. Liu has been tortured psychologically. He has been kept in confinement so that he might yield to authority after undergoing mental pressure. He is not allowed to read uncensored books or materials of his choice; he can only receive information that the authorities want him to have. By doing so, the authorities hope that they will ultimately change his values, beliefs, perceptions, judgments, and then later his mindset and behavior.

CAUSES OF ACTION

86. Plaintiffs' causes of action arise under and violate the following laws, agreements, conventions, resolutions, and treaties:

- a. Alien Tort Statute, 28 U.S.C. § 1350;
- b. Torture Victim Protection Act, 28 U.S.C. § 1350;
- c. Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment G.A. res. 39/46, annex, 39 U.N. GAOR Supp. (No. 51) at 197, U.N. Doc. A/39/51 (1984), *entered into force* June 26, 1987;
- d. International Covenant on Civil and Political Rights, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, *entered into force* Mar. 23, 1976;
- e. Universal Declaration of Human Rights (1948) G.A. res. 217A (III), U.N. Doc A/810 at 71;

- f. Charter of the United Nations (1945), adopted June 26, 1945, 59 Stat. 1031, T.S. 993, 3 Bevans 1153 (*entered into force* October 24, 1945);
- g. International Labor Organization Convention No. 29 Concerning Forced or Compulsory Labor (1930), *adopted* June 28, 1930, 39 U.N.T.S. 55 (*entered into force* May 1, 1932);
- h. The Electronic Communications Privacy Act, 18 U.S.C. § 2701, § 2702, and §2511; and
- i. Statutes and common law of the State of Maryland, including but not limited to assault and battery, false imprisonment, negligence, intentional infliction of emotional distress, negligent infliction of emotional distress, and unfair business practices.

FIRST CLAIM FOR RELIEF

(Torture, a Violation of International Law for Which the Alien Tort Statute and the Torture Victim Protection Act Provide Relief)

(By All Plaintiffs Against All Defendants)

87. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 86 of this Complaint as if fully set forth herein.

88. Defendants' acts described in this Complaint caused direct and severe physical and mental pain and suffering to the Plaintiffs and placed them at severe risk of personal injury and/or death in connection with their participation in, and support of, the peaceful exercise of their rights of free speech and communication, free association, and the right to hold, exercise and express their political beliefs.

89. Because the acts enabled by Defendants as described herein violated multiple provisions prohibiting torture on an absolute basis including: (1) treaties binding on the United

States, (2) statutes adopted by the Congress of the United States implementing those treaty obligations, (3) international and domestic judicial decisions applying and interpreting the prohibition against cruel, inhuman, or degrading treatment or punishment, (4) administrative regulations and international and domestic judicial decisions applying and interpreting the prohibition against torture, and (5) a number of specific, universal, and obligatory standards that are recognized to be part of customary international law, these acts constitute “tort[s] ... committed in violation of the law of nations or a treaty of the United States” under the Alien Tort Statute (ATS), 28 U.S.C. § 1350.

90. These acts also specifically constitute torture in violation of the Torture Victim Protection Act (TVPA), 28 U.S.C. § 1350.

91. Defendants aided and abetted and/or ratified these acts of torture in violation of international, federal, and state law. These violations and actions meet the definition of torture under the meaning of the TVPA, the ATS, and international treaties and U.S. laws and regulations, as well as customary international law, which condemn torture on an absolute basis, irrespective of the reasons why the abuses are inflicted. These violations also meet the standard for liability established by the TVPA, creating liability for anyone who “subjects”, or causes another to undergo torture.

92. Defendants knowingly violated Art. XVII of the International Covenant on Political and Civil Rights by failing to take action to prevent acts of torture. The ICCPR and customary international law establish a standard for aiding and abetting torture that requires positive steps be taken to prevent acts of torture. Defendants’ sale of products to the CCP, directly or indirectly, that they knew would be used to facilitate torture is a violation of this prohibition.

93. The Plaintiffs are therefore entitled on this basis to compensatory and punitive damages, in amounts to be established at trial, and to such other declaratory and/or injunctive relief as may be deemed appropriate.

SECOND CLAIM FOR RELIEF

**(Cruel, Inhuman or Degrading Punishment or Treatment or Punishment,
Violations of International Law for Which the Alien Tort Statute Provides Relief)**

(By All Plaintiffs Against All Defendants)

94. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 93 of this Complaint as if fully set forth herein.

95. These acts of cruel, inhuman, or degrading treatment or punishment suffered by the Plaintiffs designated in this Second Claim for Relief, including physical injury and the severe physical and mental suffering associated therewith, were inflicted upon them by the joint and collusive actions of Defendants and PRC government officials acting under color of law, through unlawful or unauthorized actions prohibited by international law.

96. These acts had the intent and the effect of grossly humiliating, debasing, intimidating, and punishing the Plaintiffs, forcing them to act against their will and conscience, inciting fear and anguish, and seeking to break their physical and/or moral resistance.

97. These acts of cruel, inhuman, or degrading treatment or punishment were inflicted on the Plaintiffs for purposes that include, among others, preventing them from exercising their free speech and free association rights, and punishing them for exercising their right to have and communicate political beliefs.

98. Because the acts described herein violated the prohibitions against cruel, inhuman, or degrading punishment or treatment including: (1) treaties binding on the United States, (2) statutes adopted by the Congress of the United States implementing those treaty

obligations, (3) international and domestic judicial decisions applying and interpreting the prohibition against cruel, inhuman, or degrading treatment or punishment, (4) administrative regulations and international and domestic judicial decisions applying and interpreting the prohibition against cruel, inhuman or degrading treatment or punishment, and (5) a number of specific, universal, and obligatory standards that are recognized to be part of customary international law, these acts constitute “tort[s] ... committed in violation of the law of nations or a treaty of the United States” under the Alien Tort Statute, 28 U.S.C. § 1350.

99. Defendants knowingly aided and abetted and/or ratified these abuses, and did not act to prevent or punish these violations of human rights as embodied in international law.

100. Defendants are liable for knowingly aiding and abetting and/or ratification of the commission of these abuses under this cause of action.

101. The Plaintiffs are therefore entitled on this basis to compensatory and punitive damages in amounts to be established at trial, and to such other declaratory and/or injunctive relief as may be deemed appropriate.

THIRD CLAIM FOR RELIEF

(Arbitrary Arrest and Prolonged Detention, a Violation of International Law for Which the Alien Tort Statute and the Torture Victim Protection Act Provide Relief)

(By All Plaintiffs Against All Defendants)

102. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 101 of this Complaint as if fully set forth herein.

103. These acts of arbitrary arrest and long-term detention suffered by the Plaintiffs designated in this Third Claim for Relief, including arrest and detention for an unlawful purpose in violation of the rights to freedom of speech, association, and assembly, were inflicted upon them by the joint and collusive actions of Defendants and government officials acting under

color of law, albeit through unlawful or unauthorized actions and for unlawful and unauthorized purposes.

104. These acts caused direct physical and mental pain and suffering upon the Plaintiffs, caused loss of liberty and property, and placed them at severe risk of personal injury in connection with their participation in, and support of, the peaceful exercise of their rights of free speech and free association, and their rights to hold, exercise, and express their political beliefs.

105. Because the acts described herein violated provisions prohibiting arbitrary arrest and prolonged detention including: (1) treaties binding on the United States, (2) statutes adopted by the Congress of the United States implementing those treaty obligations, (3) international and domestic judicial decisions applying and interpreting the prohibition against arbitrary arrest and prolonged detention, (4) administrative regulations and international and domestic judicial decisions applying and interpreting the prohibition against arbitrary arrest and prolonged detention, and (5) a number of specific, universal, and obligatory standards that are recognized to be part of customary international law, these acts constitute “tort[s] ... committed in violation of the law of nations or a treaty of the United States” under the Alien Tort Statute, 28 U.S.C. § 1350.

106. Defendants aided and abetted in the carrying out of these abuses, and did not act to prevent or punish these violations of human rights as embodied in international and domestic law.

107. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses, as specified in this cause of action.

108. The Plaintiffs are therefore entitled on this basis to compensatory and punitive damages, in amounts to be established at trial, and to such other declaratory and/or injunctive relief as may be deemed appropriate.

FOURTH CLAIM FOR RELIEF

**(Forced Labor, a Violation of International Law for Which the
Alien Tort Claims Act and the Torture Victims Protection Act Provide Relief)**

(By All Plaintiffs Against All Defendants)

109. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 108 of this Complaint as if fully set forth herein.

110. The Plaintiffs were placed in fear for their lives, were deprived of their freedom, and were forced to suffer severe physical and mental abuse associated with forcing them into working in the prison factories in inhumane conditions, by the joint and collusive actions of Defendants and government officials acting under color of law, through unlawful or unauthorized actions.

111. Because the acts described herein violated provisions prohibiting forced labor including: (1) treaties binding on the United States, (2) international and domestic judicial decisions applying and interpreting the prohibition against forced labor, and (3) administrative regulations and international and domestic judicial decisions applying and interpreting the prohibition against forced labor, and (4) a number of specific, universal, and obligatory standards that are recognized to be part of customary international law, these acts constitute “tort[s] ... committed in violation of the law of nations or a treaty of the United States” under the Alien Tort Claims Act, 28 U.S.C. § 1350.

112. Defendants aided and abetted in the carrying out of these abuses, and did not act to prevent or punish these violations of human rights as embodied in international and domestic law.

113. Defendants are liable for knowingly aiding and abetting and/or ratifying this cause of action.

114. The Plaintiffs are therefore entitled on this basis to compensatory and punitive damages to be established at trial, and to such other declaratory and/or injunctive relief as may be deemed appropriate.

FIFTH CLAIM FOR RELIEF

(Battery)

(By All Plaintiffs Against All Defendants)

115. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 114 of this Complaint as if fully set forth herein.

116. On information or belief, Defendants intentionally committed acts that resulted in harmful or offensive treatment of Plaintiffs' persons, and produced bodily harm. Plaintiffs did not consent to the contact and treatment that caused injury, damage, loss or harm to Plaintiffs.

117. The acts described constitute battery, actionable under the laws of the state of Maryland and the United States.

118. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses, as specified in this cause of action.

SIXTH CLAIM FOR RELIEF

(Assault)

(By All Plaintiffs Against All Defendants)

119. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 118 of this Complaint as if fully set forth herein.

120. On information or belief, Defendants' conduct caused Plaintiffs to be subjected to numerous assaults and/or intentional invasions of their rights to be free from offensive and harmful contact, and said conduct demonstrated that Defendants had a present ability to subject Plaintiffs to immediate, intentional, offensive and harmful touching.

121. The acts described herein constitute assault, actionable under the laws of the state of Maryland and the United States.

122. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses, as set forth in this cause of action.

SEVENTH CLAIM FOR RELIEF

(False Imprisonment)

(By All Plaintiffs Against All Defendants)

123. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 122 of this Complaint as if fully set forth herein.

124. On information or belief, Defendants intentionally and unlawfully exercised force or the express or implied threat of force to restrain, detain or confine Plaintiffs on an arbitrary and unlawful basis. The restraint, detention or confinement compelled Plaintiffs to stay or go somewhere against their will for some appreciable time. Plaintiffs did not consent to this restraint, detention or confinement.

125. Defendants' actions constituted false imprisonment under standards of law applied by the state of Maryland and the United States.

126. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses as specified in this cause of action.

EIGHTH CLAIM FOR RELIEF

(Intentional Infliction of Emotional Distress)

(By All Plaintiffs Against All Defendants)

127. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 126 of this Complaint as if fully set forth herein.

128. On information or belief, Defendants intended to cause Plaintiffs to suffer emotional distress, or, in the alternative, (a) Defendants engaged in the conduct adversely affecting Plaintiffs with reckless disregard of the high probability that it would cause Plaintiffs to suffer severe abuses and emotional distress, (b) Plaintiffs were present at the time the outrageous conduct and these results occurred and (c) Defendants knew that Plaintiffs were present and would be adversely affected.

129. Plaintiffs suffered severe abuse and emotional distress as a result of the conduct of Defendants.

130. Defendants' conduct constitutes the intentional infliction of emotional distress and is actionable under the laws, standards, and causes of action of the State of Maryland and the United States.

131. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses as set forth in this cause of action.

NINTH CLAIM FOR RELIEF

(Negligence)

(By All Plaintiffs Against All Defendants)

132. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 131 of this Complaint as if fully set forth herein.

133. On information or belief, Defendants failed to use ordinary or reasonable care in order to avoid injury to Plaintiffs. Defendants' negligence was a cause of injury, damage, loss or harm to Plaintiffs.

134. As a result of these acts, Plaintiffs suffered harm including, but not limited to, severe emotional distress. Defendants' conduct constitutes negligence and is actionable under the causes of action of the State of Maryland and the United States.

135. Defendants are liable for knowingly aiding and abetting and/or ratifying these abuses as specified in this cause of action.

TENTH CLAIM FOR RELIEF

**(Violation of the Electronic Communications Privacy Act,
18 U.S.C. § 2701, §2702, and §2511, Unlawful Access to Stored Communications)**

(By All Plaintiffs Against All Defendants)

136. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 135 of this Complaint as if fully set forth herein.

137. Upon information and belief, Defendants violated the rights of Plaintiffs herein by intercepting, disclosing, and/or intentionally using electronic communication between Plaintiffs and other persons. The right of a civil action arises under 18 U.S.C. 2707(a), which provides that any person aggrieved by any violation of the Electronic Communications Privacy Act, “in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind

may, in a civil action, recover from any person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.”

138. Defendants exceeded their authorization to access and control private information concerning Plaintiffs’ electronic communications, in violation of 18 U.S.C. § 2701.

139. Defendants unlawfully and knowingly divulged Plaintiffs’ electronic communication contents and user information, in violation of 18 U.S.C. § 2702.

140. Defendants knowingly aided and abetted the intentional and unlawful acquisition and/or interception of electronic communications sent by and/or received by Plaintiffs through the use of an electronic device. Defendants aided and abetted the intentional and unlawful acquisition and/or interception of communications that had been sent from or directed to Plaintiffs through their use of computers and other electronic devices which were part of, and utilized in, Defendants’ electronic communications system, in violation of 18 U.S.C. § 2511 and pursuant to 18 U.S.C. § 2520.

141. Defendants knowingly aided and abetted the unlawful access, use, and disclosure of Plaintiff’s intercepted communications to enhance their business in China. This disclosure was not necessary for the operation of Defendants’ system or to protect Defendants’ rights or property.

142. Plaintiffs are “person[s] whose ... electronic communication is intercepted ... or intentionally used in violation of this chapter” within the meaning of 18 U.S.C. § 2520.

143. Defendants are liable directly and/or vicariously for this cause of action.

144. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages

consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

ELEVENTH CLAIM FOR RELIEF

(Arbitrary Interference with the Right to Privacy, a Violation of International Law and Art. XVII of the International Covenant on Civil and Political Rights for Which the Alien Tort Statute Provides Relief)

(By All Plaintiffs Against All Defendants)

145. Plaintiffs re-allege and incorporate by reference the facts and allegations set forth in paragraphs 1 through 144 of this Complaint as if fully set forth herein.

146. Upon information and belief, Defendants violated the rights of Plaintiffs herein by subjecting them to arbitrary or unlawful interference with their privacy, family, home or correspondence. These gross violations of the individuals' privacy were inflicted upon them by the joint and collusive actions of Defendants and PRC government officials acting under color of law, through unlawful or unauthorized actions prohibited by international law.

147. These privacy violations were inflicted on the Plaintiffs for purposes that include, among others, preventing them from exercising their free speech and free association rights, and punishing them for exercising their right to have and communicate political beliefs.

148. Because the acts described herein violated the prohibitions against arbitrary interference with an individual's privacy including: (1) treaties binding on the United States, (2) statutes adopted by the Congress of the United States implementing those treaty obligations, (3) international and domestic judicial decisions applying and interpreting the prohibition against arbitrary interference with individual privacy (4) administrative regulations and international and domestic judicial decisions applying and interpreting the prohibition against arbitrary interference with individual privacy and (5) a number of specific, universal, and obligatory

standards that are recognized to be part of customary international law, these acts constitute “tort[s] ... committed in violation of the law of nations or a treaty of the United States” under the Alien Tort Statute, 28 U.S.C. § 1350.

149. Defendants knowingly aided and abetted and/or ratified these abuses, and did not act to prevent or punish these violations of human rights as embodied in international law.

150. Defendants are liable for aiding and abetting and/or ratification of the commission of these abuses under this cause of action.

151. The Plaintiffs are therefore entitled on this basis to compensatory and punitive damages in amounts to be established at trial, and to such other declaratory and/or injunctive relief as may be deemed appropriate.

ABSENCE OF AVAILABLE AND EFFECTIVE REMEDIES IN CHINA

152. There is no adequate alternative remedy available in China to Plaintiffs for the claims asserted here.

153. Chinese attorneys have been disbarred, arrested, and persecuted for their attempts to defend dissident Chinese internet users in Chinese courts. Plaintiffs residing outside of China cannot return to China without danger of serious reprisals, nor can those residing inside China bring suit without danger of serious reprisals.

154. The Chinese judiciary or legal system does not operate independent of other branches of government and/or of the CCP in China.

155. Plaintiffs still detained continue to suffer from beatings, sleep and food deprivation, and other forms of torture, cruel, inhuman, or degrading treatment, forced labor, and crimes against humanity.

156. Plaintiff under surveillance or house arrest continue to have their freedom of movement, expression, and association restricted and their privacy invaded.

157. Technologies and other measures used to suppress dissident Chinese internet users in China make it virtually impossible for plaintiffs to bring cases in China without reprisal and further persecution of them and their families. In addition, it is virtually impossible for detained dissident Chinese internet users to bring cases in any foreign courts.

158. Many dissident Chinese internet users in China have attempted to seek administrative remedies against responsible Chinese CCP or State officers. This has resulted in further retaliation against them, including renewed detention, increased persecution, and “disappearance”.

STATEMENT PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 11(b)(3)

159. Due to the unique circumstances of this case, specifically the fact that a substantial amount of the information is unavailable without Defendants’ cooperation, the factual allegations in paragraphs 45, 51, 120, 124, 128, 133, 137, 146 are made because they “are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery,” pursuant to Rule 11(b)(3). Fed. R. Civ. P. 11(b)(3).

PRAYER FOR RELIEF

160. WHEREFORE, the Plaintiffs pray for judgment against Defendants, as follows:

- a. For actual and compensatory damages to each of the Plaintiffs according to proof to be established at trial;
- b. For punitive and exemplary damages according to proof to be established at trial;

- c. For declaratory relief determining that the actions of Defendants constituted violations of international law, specifically, that such violations included prohibited acts of torture, cruel, inhuman or degrading treatment, and arbitrary arrest and prolonged detention for the peaceful and exchange of ideas, views, and political beliefs in violation of the Convention Against Torture, numerous other international treaty obligations binding on the United States, and domestic laws and regulations implementing such standards, including the Torture Victim Protection Act, and other enumerated causes of action in this Complaint;
- d. For affirmative action by Defendants to secure the release of the detainees;
- e. For such other relief as the Court deems just and proper.

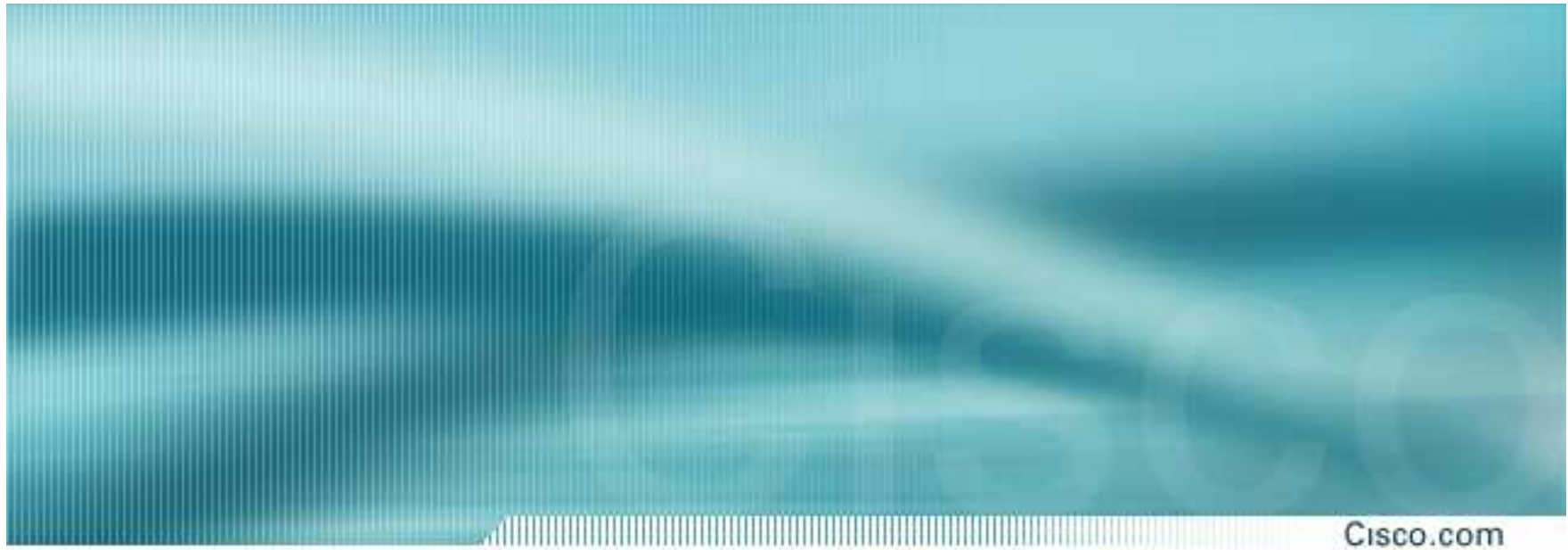
Respectfully Submitted,

June 6, 2011

/s/ Daniel S. Ward
Daniel S. Ward
Ward & Ward, P.L.L.C.
2020 N Street, NW
Washington D.C. 20036
(202) 331-8160
(202) 503-1455 (facsimile)
dan@wardlawdc.com
Counsel for Plaintiffs

With the assistance of:
Shaun Kern, Jaime Cardenas-Navia,
and Alec Wright
Georgetown University
Law Center
Legal Clerks

EXHIBIT A



Overview of the Public Security Sector

Agenda

Cisco.com

- 1. Organizational Structure**
- 2. PS Services & Police Reform**
- 3. Current Status of Information Communication**
- 4. The Golden Shield Project**
- 5. Challenges of the Industry**

Ministry of Public Security

Cisco.com

Bureau 1 (Domestic Security Protection Bureau), Bureau 2 (Economic Crimes Investigation Bureau), Bureau 3 (Public Security Management Bureau), Bureau 4 (Border Control Bureau), Bureau 5 (Criminal Crimes Investigation Bureau), Bureau 6 (Border Entry & Exit Affairs Bureau), Bureau 7 (Firefighting Bureau), Bureau 8 (Security Guard Bureau), Bureau 9 (Central Gov. Security Guard Bureau), Bureau 10 (PS Bureau of the Ministry of Railways), Bureau 11 (Public Information & Network Security Supervision Bureau), Bureau 12 (Action & Technology Bureau), Bureau 13 (Jails Management Bureau), Bureau 14 (PS Bureau of the Ministry of Communications), Bureau 15 (PS Bureau of CAAC), Bureau 16 (PS Bureau of the National Forestry Administration), Bureau 17 (Traffic Administration Bureau), Bureau 18 (Legal Affairs Bureau), Bureau 19 (Foreign Affairs Bureau), Bureau 20 (Equipment & Financial Bureau), Bureau 21 (Anti-Narcotics Bureau), Bureau 22 (Science & Technology Bureau), Bureau 23 (Information & Communication Bureau), Bureau 24 (Smuggling Crimes Investigation Bureau)

The Ministry of Public Security has bureau level organizations including the General Office, Police Affairs Supervision, Personnel & Training, Publicity, Domestic Security Protection, Economic Crimes Investigation, Public Security Management, Border Control, Criminal Crimes Investigation, Border Entry & Exit, Firefighting, Security Guard, Public Information & Network Security Supervision, Jails Management, Traffic Administration, Legal Affairs, Foreign Affairs, Equipment & Finance, Anti-Narcotics, Science & Technology, and Information & Communication.

The PS bureaus of railway, traffic, civil aviation, forestry, and smuggling crimes investigation are included in the Ministry of Public Security, but are subject to the dual leadership of the respective governing authorities and the Ministry of Public Security.

(China used to treat terrorist cases as serious criminal cases in the past, so such cases were mainly handled by the criminal affairs police, and the first section/unit of the PS bureaus at different levels (Officially called: Domestic Security Protection Section/Unit, which formerly known as Political Security Protection Section/Unit) was responsible for intelligence support)

Beijing Municipal Public Security Bureau

Cisco.com

1. Criminal Investigation Brigade
2. Firefighting Bureau
3. State Security Protection Brigade
4. PS Brigade
5. Population Management Section
6. Action & Technology Section
7. Office of Technical Measures for Security Protection
8. Culture Protection Section
9. Patrol Police Brigade
10. Public Transportation Sub-bureau
11. Security Guard Bureau
12. Security Protection Section
13. Internal Security Protection Bureau
14. Border Entry & Exit Administration Section
15. Economic Investigation Section
16. Anti-riot & Security Detection Section
17. Traffic Administration
18. Supervision Section
19. Headquarters of the bureau
20. Information Center
21. Monitoring Center
22. Command Center
23. Ankang Hospital
24. Public Security Hospital
25. Police Academy
26. The Second Police School

The Criminal Investigation Brigade (The SWAT Team): Recreated on the basis of the former Criminal Investigation Section, Pre-interrogation Section, Anti-Narcotics Section and SWAT Team of the Beijing Municipal Public Security Bureau

Beijing Traffic Management Bureau

Cisco.com

It is under the leadership of the Beijing Municipal Public Security Bureau, has 22 business sections & offices, and has traffic detachments (brigades) in 18 districts (counties), the Capital Airport, and the Yizhuang Economic Development Zone

Beijing Fire Fighting Bureau

Cisco.com

Beijing Fire Fighting Bureau

**The Beijing Fire Fighting Brigade of the Chinese People's Armed Police
Beijing Public Security Bureau Fire Fighting Brigade**

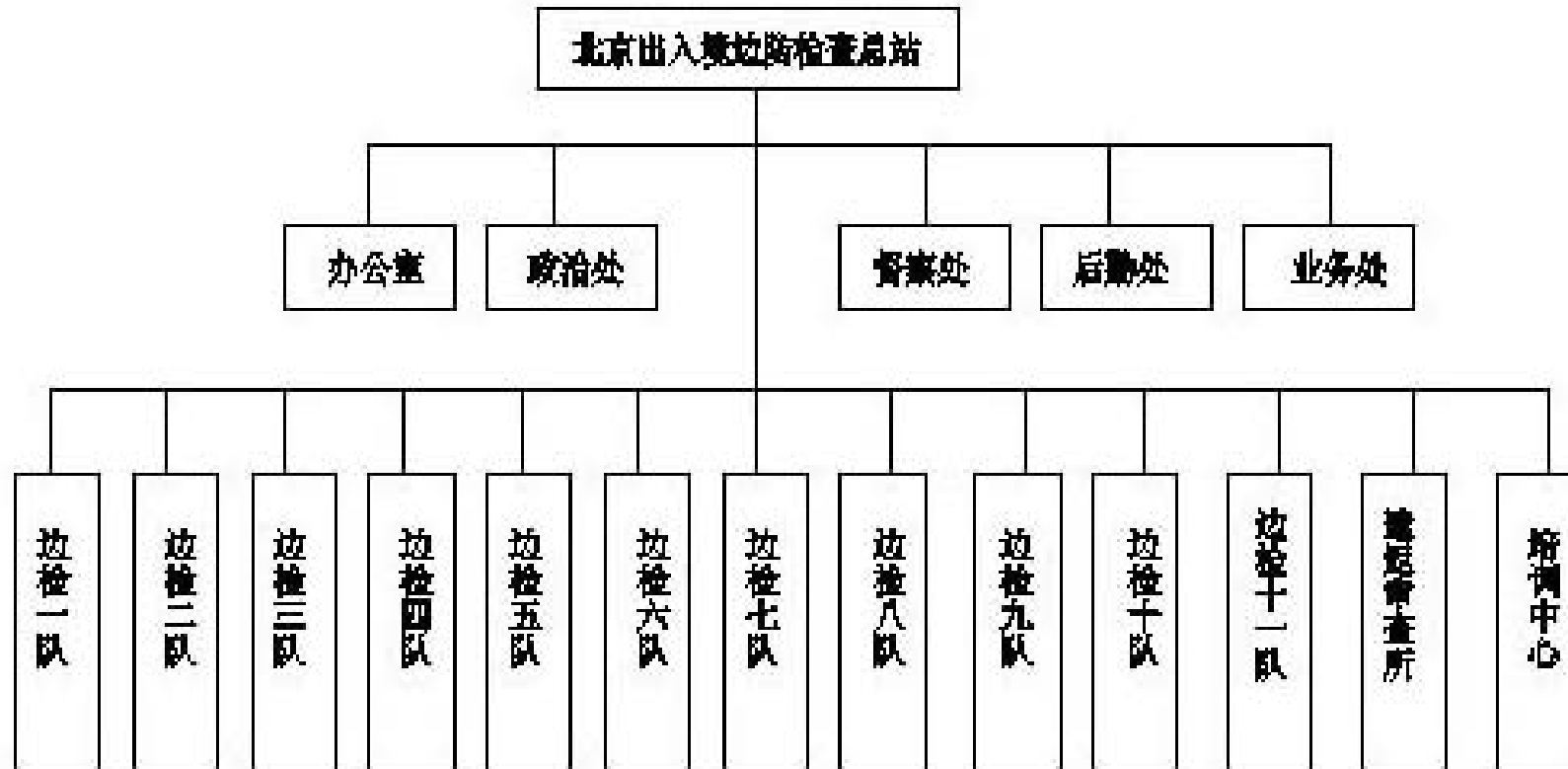
**The Fire Fighting Bureau has four units: The Command Office, the
Political Unit, the Logistics Unit, and the Fire Prevention Unit**

**The four units has 29 business sections/offices and 3 direct
subordinate organizations—the Guiding Brigade, the Hospital and the
Training Center (no official staff treatment yet)**

The entire city has a total of 44 detachments

Beijing Border Check Station

Cisco.com



In May 1988, Beijing Border Check Station and the Border Control Bureau of the Beijing Municipal Public Security Bureau were merged to become a single organization, which was called the Border Control Bureau of the Beijing Municipal Public Security Bureau internally and Beijing Border Check Station externally.

In Jan 1, 1998, in accordance with the Approval Opinions of the State Council on the Pilot Reform of the Professionalization of Border Check in Nine Cities Including Beijing, on the basis of the Border Control Bureau of the Beijing Municipal Public Security Bureau, the Beijing Entry & Exit Border Check Station was set up, directly reporting to the **Entry & Exit Administration Bureau of the Ministry of Public Security**.

© 2002, Cisco Systems, Inc. All rights reserved.

Cisco Systems, Inc. Confidential

Tianjin Public Security Border Control Brigade

Cisco.com

**Border check stations in Zhang Guizhang, Tanggu,
Nanjiang, and Donggang
Marine Police Branch
Guiding Brigade
Border Control Branch**

**Since 1998, the focus of the Border Control Brigade
has been shifted to:**

**Fighting cross-border criminal activities such as
illegal immigration, smuggling, and traffickering of
weapons and drugs**

Different Organizations

Cisco.com

Grass-root PS organizations:

Local police stations, criminal police units in charge of specific areas, police affairs studios (station), firefighting brigades, traffic teams (accidents sections, law enforcement stations), vehicles administration offices, patrol police squads, security police squads

Security protection councils of towns, joint security protection squads in rural areas , security check stations, border check stations

Local police stations: local police stations for security/ local police stations for household registration (can also in charge of security) /police stations in border areas (population, security)

Community police service: community police, security police, internal affairs police

Local police stations: 30 thousand; 2500 in Jiangsu province

Border control brigade, detachments, border check stations, border workstations, and border police stations

Brigade (firefighting, traffic police, patrol police, criminal police, public security, anti-narcotics, economic investigation, action technologies) /branch squads /detachments (battalions or companies)

Custody stations, jails (1-6 months), security custody stations, rehabilitation centers for drugs users, forced custody & education centers, and Ankang Hospitals

Law enforcement: prisons (0.5-20 years), forced labor (1-3 years)

Civil affairs: forced custody and repatriation centers

PS in Different Industries

Cisco.com

- **Railways**
- **Transportation**
- **Civil Aviation**
- **Forestry**
- **Smuggling Crimes Investigation Bureau**

The Political & Legal Affairs Commission

Cisco.com

- **The Political & Legal Affairs Commission (integrated management office, population office, office for fighting against smuggling, and anti-narcotics office)**
- **PS, procuratorate, court, jurisdiction, and security authorities having the law enforcement power**
- **5 subordinate organizations: court, procuratorate, public security bureau, legal affairs bureau, and civil affairs bureau**

Public security, procuratorate, court, legal affairs (prisons), national security, and armed police

Police Varieties of the Public Security System

Cisco.com

1. Security police
2. Household registration police
3. Criminal police
4. Traffic police
5. Foreign affairs police
6. Economic investigation police
7. Anti-narcotics police
8. Internet police
9. Anti-riot police
10. Legal police
11. Prison police

1. Armed police
2. Border police
3. Firefighting police
4. Security guard police
5. Railway police
6. Anti-smuggling police
7. Navigation police
8. Civil aviation police
9. Forest police

1. Special police
2. Water police
3. Traffic & patrol police
4. Air police

The armed police has eight varieties of police forces in three categories

Cisco.com

Category one, internal security protection force: under the direct leadership of the head office of the armed police

14 mobile divisions: code-named 8610, 8620, 8630, 8640, 8650, 8660, 8670, 8680, 8690, 8710, 8720, 8730, 8740, and 8750.

Category two, under the dual leadership of related governing agencies of the State Council and the head office of the armed police

The gold force, the hydro-electric force, the transportation force, and the forest force

Category three, under the leadership of the public security authority

The border force: The border control bureau administers border check, border patrol, and sea-based smuggling control

The firefighting force: Under the administration of the firefighting bureau, implementing fire prevention and fire fighting tasks

The security guard force: Under the administration of the security guard bureau, responsible for the security guard of the Party and state leaders, main provincial & city leaders, as well as the visiting foreign dignitaries

Overview of the Police Force Nationwide

Cisco.com

1.60 million police, 10.86 per ten thousand people; 35 per ten thousand people in developed countries

Local police stations: 380 thousand

Traffic police: More than 200 thousand, 1.2 traffic police/kilometer of highway

Criminal police: 150 thousand

Firefighting police (armed police): 120 thousand

Patrol & anti-riot police squads: 80 thousand; the “110” police is responsible for both anti-riot tasks and patrolling

Information & communication police: 16,000

Confidential staff: 10 thousand

Guangdong: 120 thousand Jiangsu: 70 thousand Beijing: 30 thousand

Overview of the Police Force Nationwide

Cisco.com

Over the past 20 years, more than 6 thousand police officers died at work and 100 thousand were injured across the country.

“There is blood shedding every moment, and there is sacrifice everyday”

The frontline police officers work 11 to 15 hours a day on average

In 2001 more than 450 police officers died at work in China, whereas the number was just 2 in Japan in the same year

In 2001, among the 458 died, 148 died at work due to long-time overwork, accounting for 33.4%; 68 died of attack from criminals; 204 died of traffic accidents, accounting for 46%; and 38 died in the process of pursuing criminals

The percentage of police in the total population is the lowest for the Chinese police, their salary is also the lowest in the world, but their workload is the biggest in the world

Opportunities for Cisco: Levels 1, 2, 3 and 4 Networks

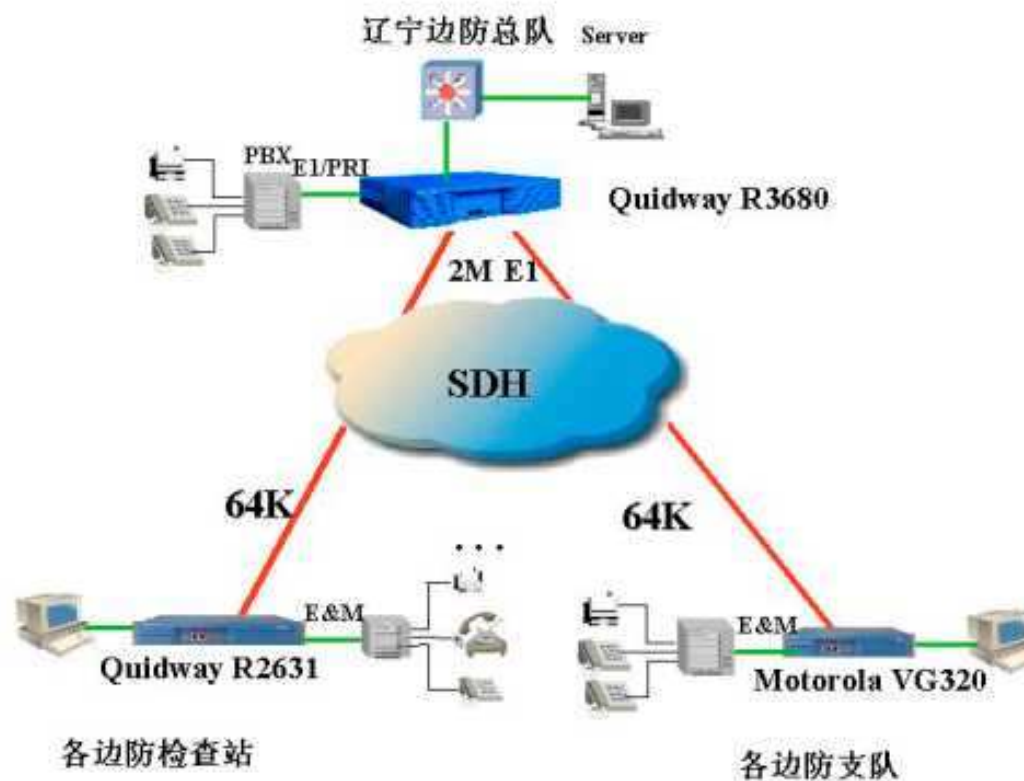
Cisco.com

- **Traffic management**
- **Firefighting**
- **Border control**
- **Legal affairs network**

Liaoning Border Control Network

Cisco.com

辽宁边防组网图



Agenda

Cisco.com

- 1. Organizational Structure**
- 2. PS Services & Police Reform**
- 3. Information & Communication Status**
- 4. The Golden Shield Project**
- 5. Challenges of the Industry**

Police Services

Cisco.com

1. Security management
2. Household registration management
3. Traffic management
4. Legal affairs
5. Economic investigation
6. Criminal investigation
7. Border management
8. Firefighting management
9. 110 patrol police
10. Narcotics confiscation and control
11. Police service supervision
12. Anti-smuggling police
13. Foreign affairs management
14. Science & technology safety
15. Border entry & exit management
16. Complaints handling
17. Internet monitoring & supervision

Jia Chunwang 11.20 [Government Statement of Goals by Jia Chunwang]

Cisco.com

- Give top priority to maintaining **stability**, and further improve and enhance domestic security protection
- Stick to the principle of getting tough on the criminals, and substantially improve our **skills and levels** in fighting criminal activities
- Focus on the development of the public security prevention & protection system, and combine the **rigorous enforcement, rigorous control, rigorous prevention, and rigorous management** organically together
- Further reform and enhance the **public administration work of the PS system**
- Reform the **PS management systems and public service assurance mechanisms** based on the simplified, unified, and effective principle
- The development of the Party's system and the **police force** in the PS sector

The Four Principles Related to Police Management

Cisco.com

- **Developing the police force with an awareness of government policy goals**
- **Managing the police force in accordance with law**
- **Building up the capacity of the police force with technology: information, criminal investigation, action**
- **Culture education for the police**

Features of the PS Sector: Law Enforcement Goal

Cisco.com

- **Unified command**
- **Fast reaction**
- **Concerted action**

Three Major Strategies for Local Police Stations

Cisco.com

- **Information strategy**
- **Community police service strategy**
- **Standardization strategy**

Role Models in the PS Sector

Cisco.com

- **Jinan Traffic Police: A flag in the country's PS sector**
"Rigorous law enforcement, warm services"—Jiang Zemin
- **Zhangzhou 110:**
Police call command & dispatching system
- **Benxi Municipal Public Security Bureau:**
Improving the quality and capacity of the police force through internal reform

The Fifth Squad of the traffic & patrol police in Yangpu was named "Xiao Yuquan Detachment" by the Shanghai Municipal Public Security Bureau; respect ones job and caring for the people

Police Reform

Cisco.com

- 1. Criminal investigation**
- 2. Traffic & Patrol Police**
- 3. Administration Reform**
- 4. Introduce Community-based Police Services**

Reform in Criminal Investigation

Cisco.com

On June 9, 1997, the Ministry of Public Security convened the National Working Conference on Criminal investigation in Shijiazhuang, Hebei Province, and made the decision to initiate reform in criminal investigation in the country's PS sector

**Based on the criminal police squad responsible for a specific area
Investigation & interrogation combined together
Accountability system in criminal investigation
New mechanisms for cracking down on criminal activities
Criminal investigation information system
Training for all the criminal police officers**

Enhancing the technology awareness, and promoting the adoption of IT and other modern technologies in criminal investigation activities

Reform of Traffic & Patrol Police

Cisco.com

In the past, there was only one variety of police, there were too many law enforcement processes and there was a waste of the police force

“Simplifying the head office, enriching the grass-root, improving efficiency, and enabling one police officer to have multiple skills”

The new traffic & patrol police: one police with multiple law enforcement tasks; improved police services

In the past: criminal activities were not able to be cracked down thoroughly; a case might be accepted, but might not be handled or handled by two different police teams at the same time; lack of accountability among different police teams

**Shanghai Municipality
Tieling, Liaoning**

Administration Reform

Cisco.com

- **Transparency in police services, “sunshine operation”**
- **Simplifying service processes**
- **Reducing intermediate processes**
- **Shortening the time needed for a service**
- **Improving efficiency**

The Four Revolutions in Police Services

Cisco.com

Specialization: The signature of the first revolution in police services

Marked by the modernization of the police force in Greater London, UK, in 1829,

Professionalization: The core at the second revolution of police services

Marked by the professionalization of the American police at the end of the 19th century and the beginning of the 20th century

Equipment modernization: Characteristic of the third police revolution in police services

Marked by the modernization of police equipment, the dramatic improvement of the police capacity, and the emphasis on quick reaction in European and North American countries in 1930-70s

Community police services: The cornerstone of the fourth revolution in police services, from 1970s until today

The slogan of the community police services in the United States: “Let’s create miracles together”

Community Police Services: the Basic Direction of Police Service Reform in Different Countries Today

Cisco.com

1997, Suzhou, Shijiazhuang Conferences, promotion

Mar, 2002, Hangzhou, Conference of Local Police Stations, three major strategies

Before the end of 2004, in major cities around the country, one police officer is responsible for the local administration [of law enforcement] for 1000 households or 3000 people; one police officer in one community or several police officers in one community; police service strategy: based on prevention and focused on eliminating the root causes of crimes

Working goal:

Low crimes, good social order, stable society, and satisfaction of the public

To eventually realize the shift of police work:

From enforcement to prevention,

From being passive to being proactive,

And from being administration-oriented to being service-oriented

Luo Feng, Vice Minister, Ministry of Public Security, November 25, Nanjing, International Workshop

In the future, the Ministry of Public Security will further increase efforts to reform police services in communities, to be based in communities, to serve the communities, to optimize police force arrangement, to regulate police operation, and to gradually create a mechanism for community police services operation that is in line with the management system of the new types of communities

24X7 Police Services

Cisco.com

- **Patrol vehicles, fixed posts, and mobile posts**
- **Points (police posts, police offices)**
- **Lines (patrol lines)**
- **Areas (communities)**

Opportunities for Cisco

Cisco.com

- **Trends**
- **Industry Hotspots**
- **Service Assurance (BW, QoS/Security)**

Agenda

Cisco.com

1. Organizational Structure
2. PS Services & Police Reform
3. Current status of Information & Communication
4. The Golden Shield Project
5. Challenges of the Industry

Information System Status: Wired Communication Network for Telephone (1)

Cisco.com

Head office of the Ministry: Siemens 350, 4 E1 relay lines and 150 E&M relay lines, with satellite line serving as the backup line for the primary network

- **Primary network: 3-6 lines**
- **Primary network: 1-4 lines**
- **Tertiary network: 1-3 lines**

- **Long-distance telephone, tele-conferencing, text fax, photo fax, password-protected telegram**

Information System Status: Wired Communication Network for Data (2)

Cisco.com

Mainly relying on the digital lines rented from China Telecom and the communication arm of the Headquarters of the General Staff of the PLA, supported by the exclusive satellite channels for public security

Primary network: $N*2M$ ($1 \leq N \leq 3$)

Information Center of the Ministry: two units of CISCO 7507

Current Situation of Information System: Confidential Communication (3)

Cisco.com

Encryption Work Steering Group of Ministry of Public Security
(**Confidential Affairs Bureau** of General Office of the State Council)

All levels higher than region-city

All counties except for Tibet

Level 1 and 2 networks: Encrypted communication network for **core encrypted fax**

Level 3 network: Encrypted communication network for **common encrypted fax**

Ministries, province (autonomous region and municipals) and “Two Offices”

Internal protection, border guard, borders inspection and guard

Encrypted communication: life line, security line and command line

Millions of encrypted telegram and messages per year

Current Situation of Information System: Wireless and Mobile Communication (4)

Cisco.com

Distributed mobile network: 30KM Fixed point link network, Emergency Command Network: 100KM

Band dedicated for Public Security System:

VHF-D, S: Band for 150M network

UHF-P: Band for 360M network

UHF-E: 460M link frequency, band for supplementary network

UHF: Band for 800M network

- Basic 150M for public security: paging interference is severe, still being used in some small city and counties as well as in rural areas

Remote areas: short-wave network, certain public security organs: paging system

- Functional 360M for public security: guard, transportation and reconnaissance, small in number
- Automatic GA176 for public security (enhancement to MPT-1327)

Over 300 360M base station; over 2000 channels; over 80000 sets of mobile devices

Shanghai: TETRA Digital Cluster

CDPD, GPRS

Issue: Mobile data transmission and internetworking

Current Situation of Information System: Image Communication (5)

Cisco.com

TV monitoring system:

Beijing cameras: 4000, between: 16-way switching

Public security: 500 Traffic administration: 1000

**Airport: 2000 West Railway Station: 200 Beijing Station:
200**

1-core optical fiber 8 signal inputs

Video and audio conference system:

H.320 from ZTE

Using satellite communication platform for public security

Shandong: VTEL H.320

Current Situation of Information System: Satellite Communication (6)

Cisco.com

**Joint Communication Network of Ministry of Public
Security and Ministry of State Security**

Use Ku band

Transponder bandwidth: 27 M

Support 16k voice, 9.6k fax and in-band data

**Point-to-point transparent data transmission from
9.6 to 64k**

Broadcast and image transmission above 2M

Current Situation of Information System: Microwave and Short wave Communication (7)

Cisco.com

**Microwave communication:
Guangdong: Ericsson 800M
Jiangsu, Henan: Harris 2G**

**Short wave communication:
Remote mountainous areas**

Current Situation of Information System: 110 Alarming, Commanding and Scheduling Communication (8)

Cisco.com

Networking of alarming systems:

110, 119, 122

Important places

Key venues

Residence communities in cities, etc.

**Commanding Communication and Scheduling
System:**

Wireline, wireless, satellite and computer, etc.

Current Situation of Information System: Emergency Communication (9)

Cisco.com

**Communication Assurance in the event of emergency
Temporary networking (wireless)**

**Transceiver station, mobile communication vehicle (GPS
positioning)**

**In vehicles, airplanes and ships, etc. Set command post in
battle areas**

A wide range of interfaces: E&M, E1, RJ11, RJ45, V.35

**Common (150M), clustered (360M), VSAT, integrated
communication**

Current Situation of Information System: Application System

Cisco.com

High level of application in Security, criminal investigation, traffic administration, border entry & exit administration

By 2001:

Over 30000 local police stations achieved computer-based population information management

Nearly 1.1 billion persons have been registered in computer system

Information of over 600 millions persons in 255 cities is available on web site of Ministry of Public Security

About 170000 escaped criminals were arrested in 1999 through "Online Criminal Pursuing"

With respect to border entry & exit management, all passport issuing offices and border

inspection sites have implemented computer-based management

When it comes to Traffic management, information of over 30 million vehicles and about

7000 drivers is management in computer and is available on Internet throughout the country .

Current Situation of Information System: Application System

Cisco.com

- 1. Foreign-related Information Management System**
- 2. Taiwanese Entry Information Management System**
- 3. Criminal Information Management System**
- 4. Population Information Management System**
- 5. Government Insurance Information Management System**
- 6. Computer-based Portrait Combination System**
- 7. Fire Statistic Information System**
- 8. Road Traffic Accidents Information Management System**

Current Situation of Information System : CCIC

Cisco.com

Criminal Information Center
3 Levels: Ministry, Province and City
Stolen or Robbed vehicles
Escaped criminals
Stolen, robbed or missing guns

Current Situation of Information System: Online Applications

Cisco.com

- **Online Escaped Criminal Pursuing**
- **Online anti-human trafficking**
- **Remote Fingerprint comparison**
- **Ballistic Verification**
- **Image Recognition**
- **DNA Query**

Cisco's Opportunities

Cisco.com

- **Compatibility**
- **Development**
- **Quality Assurance**

Agenda

Cisco.com

- 1. Organizational Structure**
- 2. PS Services & Police Reform**
- 3. Information & Communication Status**
- 4. The Golden Shield Project**
- 5. Challenges of the Industry**

National Public Security “The Golden Shield Project” Office Leader Working Meeting [Quotes

from Government goals]

Cisco.com

16th July

Chunwang Jia

En'tao Zhu:

Treat information system construction for public security as a **strategic and comprehensive** work

Drive **high-level planning** and **high standard construction** of “The Golden Shield Project”

Enhance high-level **scientific workforce development** and **training** on information applications for policemen

Runsen Li

Characteristics of Public Security System: The Golden Shield Project

Cisco.com

- Unified leadership, centralized planning, consistent standard and phased implementation
- Phase I (2001-2003), Phase II (2004-2005)

1. Focus on “Application” and “Benefit”
2. Underlying works first
3. Insist on Innovation

Application as soul and network as foundation

**Digitalization and networking represent future direction
of security protection products**

Features of Public Security Industry: The Golden Shield Project

Cisco.com

- 1. Information Network**
- 2. Application System**
- 3. Standard Specification System**
- 4. Safety Control System**
- 5. Operation Management System**
- 6. Public Network Information Security Monitor System**

The Golden Shield Project: Information Network

Cisco.com

- **Stage 1 Project:** All public security organs at prefecture level or above, 50% public security organs at county level, 10% grassroots public security units (division, station, brigade) and 40% grassroots units will be available with dial-up networking.
- **Stage 2 Project:** It is expected that 98% public security organs at county level and 40% grassroots public security units will be available with leased circuit connection, another 2% public security organs and 60% grassroots units will also be available with dial-up networking.

The Golden Shield Project: Application System

Cisco.com

- **Stage 1 Project:**
 - Population Information Management System**
 - Criminal Investigation Information System**
 - Entry & Exit Administration Information System**
 - Watch & Control Information System**
 - Traffic Management Information System**
 - Drug Prohibition Information System**
 - Office Information Management System**
 - National Public Security Quick Search Comprehensive Information System**
(including China Criminal Information Center)
 - Public Security Commanding Center**
 - Mobile Communication** Commanding & Dispatching System
 - Publicize **Mobile End** Gradually
 - Security Videoconference and Major & Key Criminal Cases Coordinating Conference**
 - Remote Public Security Service Training & Teaching System**
 - National Public Information Network Security Control Center**
- **Stage 2 Project: Other public security service application systems, realizing the sharing of service information regarding national public security organs' services**

The Golden Shield Project: Standard Specification System

Cisco.com

- **Coding Standards for Terminologies & Vocabularies, etc.**
- **Standards for Information Processing and Exchanging**
- **Standards Regarding Data Communication Network**
- **Standards for Reliability & Maintainability**
- **Standards for Safety & Electromagnetic Compatibility**
- **Standards for Engineering & Quality Control**
- **Public Security Service Processing Process**
- **Response Time for Inquiry Log-on**

Total of 1272 items

The Golden Shield Project: Safety Control System

Cisco.com

- **Stage 1 Project: Establish structural model of engineering security system”**
- **Take security, performance, practicality, convenience and easy management, etc. into consideration**
- **Reliability indicator, fault tolerance & fault recovery, disaster tolerance & disaster recovery**
- **Network security & system security**
- **System security, network management security, internal network resource protection,**
- **Network interconnection and user access, security management and monitor, etc.**
- **Computer system security, PKI , CA certification**

The Golden Shield Project: Operation Management System

Cisco.com

- **Operation mechanism**
- **Management Mode**
- **Rules and Regulations**
- **Technical Standards & Specifications**
- **Talent Cultivation**
- **Related Technical Systems**

The Golden Shield Project: Public Network Information Security Monitor System

Cisco.com

- **Stop the network-related crimes**
- **Guarantee the security and services of public network**
- **Combat “Falun Gong” evil religion and other hostiles**

[Note: Statement of Government goals from speech government official Li Runsen]

Cisco Opportunities

Cisco.com

- **High starting point planning**
- **High standard construction**
- **Technical training**
- **Security, operational maintenance**

Agenda

Cisco.com

- 1. Organizational Structure**
- 2. PS Services & Police Reform**
- 3. Information & Communication Status**
- 4. The Golden Shield Project**
- 5. Challenges of the Industry**

Challenges Facing Public Security Organs

Cisco.com

- 1. Challenge from new economic era**
- 2. Challenge from system shift & society transition**
- 3. Challenge from entry of WTO**
- 4. Challenge from “westernize”, “Differentiation”**
- 5. Challenge from transition from rule of man to rule of law**
- 6. Challenge from world police affair revolution**
- 7. Challenge from the 4th Criminal Peak in China**
- 8. Challenge from relationship between police and other people**

Challenges Facing Public Security Organs

Cisco.com

- **Insufficient police strength**
- **Increase of floating population & unemployment population**
- **High-tech crimes**
- **Challenge from entry of WTO**

Challenges Facing Public Security Organs: Insufficient Police Strength

Cisco.com

**1.6 million policemen, accounting for 11/10000,
which is 35/10000 in developed countries**

Police strength of institution: 66.5%

Police strength of grassroots unit: 33.5%

- 1. Gain police strength from science & technology**
- 2. Gain police strength from quality improvement**
- 3. Gain police strength from management**
- 4. Gain police strength from renovation**

Gain Police Strength from Science & Technology: Challenge from information communication sector

Cisco.com

- Separate reigns in different sectors
- **Mobile case handling**
- Prevention & control system of public security
- Community police affairs
- **Urban emergency responding center**

Mobile case handling

Cisco.com

- **110 police car, 110 emergency police affair car**
- **Prowl car (110, 122)**
- **Incident handling car**
- **Emergency communication car**
- **Commanding & dispatching car**



CDPD

Cisco.com

- **Beijing, Shanghai, Guangzhou, Shenzhen, Changsha, Xiamen**
- **CDPD comprises 3 parts: equipment to be provided by Lucent**
Mobile Data Base Station (MDBS)
Mobile Data Intermediate System (MDIS)
Mobile End System (MES)

TCP/IP-based

19.2K, about 10k actual transmission rate

Allows for a transmission rate of more than 100km/h

Access air link by means of DSMA/CD

Terminal interface: RS232, PCMCIA

**Permanent population, temporary population and wander away
population**

Drivers, motor vehicles, lost vehicles, criminal at large

Beijing: more than 400 iPAQs 10 thousand yuan/set 6000+4000 (card)

GPRS

Cisco.com

SGSN: Serving GPRS support node
GGSN: Gateway GPRS support node
PCU: Packet Control Units

Speed is 150Kbps, 15 times faster than GSM's 9.6Kbps

Now: actually about 40K

GPRS application of the public security system - "GPRS-police"

**By the use of portable "-police," the public security personnel
can easily search for various types of information, thus greatly improve work efficiency.**

**Beijing: Patrols can use M388 phone or PDA, and do suspicious-person check at the same time
using a mobile phone through GPRS network connected to the network of public security,
Find suspicion's information at site.**

Traffic police use mobile phones or handsets to connect to the specific GPRS network

Enter license plates, engine, driving number

then check out the illegal operation of vehicles;

Coming to drivers of the violation, Traffic police can give punishment bill immediately

And look for a driver's violation history at the time.

3G: Dynamic 384 K, static 2 M

CDMA 1X CDMA 1X (spreading rate of 1)

Cisco.com

Data transfer rate: 150K at least two times faster than GPRS

**Data security: military technology,
a high degree of confidentiality algorithm**

**Data transfer costs: utilization of the spectrum is probably
more than six times of GPRS,
the base station signal coverage is over 3 to 4 times of GPRS**

order movies or positioning services with accuracy of 5-10 meters

Cluster: TETRA and Mobile Data

Cisco.com

Shanghai TETRA: 7.2 K, the net rate of 3 K

16 base stations, expand 8, covering to skirt area

Beijing:

350M Mobile Communication System

800M simulation cluster system

Mobile Data: No handheld station

Air 19.2 K, automotive platform 9.6 K (RS232)

City Emergency Center

Cisco.com

- **110, 119, 122**
- **120, 999**
- **Electric water gas system repair**
- **Emergency relief**
- **Mayor Hotline**

Cisco Opportunities

Cisco.com

- **MPLS VPN**
- **WLAN/Mobile Router**
- **IPT/IPCC**
- **IP Video (Multicast/QoS)**
- **E-Learning**

ITS Intelligent Transportation Systems

Cisco.com

- **Traffic management System**
- **Driver Guiding System**
- **Automobile Control System**
- **Public Transport System**
- **Road Transport System**
- **Commercial Vehicle Operating System**

ITS

Cisco.com

- **Guangzhou**
- **Shenzhen**
- **Qingdao**
- **Ji'nan**
- **Shanghai**
- **Beijing**
- **Zhongshan**

ITS

Cisco.com

- **Safety: Reducing traffic accidents and property loss**
- **Economic Benefits: Ensuring travel time punctuality**
- **Environmental Protection and Reducing Energy Consumption**

Beijing : Traffic Management Comprehensive Information System

Cisco.com

**Three networks, namely Cable, Wireless and Computer Communication
And interconnected at the communication center**

Cable Network

It comprises 2nd ring and 3rd ring TV monitoring system, signal control system and comprehensive data communication system, 2000 special electric switch system and 122 alarming system, totaling 2100 pairs of core-KM optical fiber;

Wireless Network

It comprises 28 channels and 450 and 800M wireless cluster communication system covering the urban and suburb areas of Beijing. The terminals of the network includes several thousands of radios, 60 vehicle-carrying computers and 300 GPS police vehicle.

Computer Network :

It covers 186 nodes distributed in 18 counties and districts of Beijing and more than 1326 networked computers, and 3214 fixed and portable imprinters, it realizes the networking of information center, traffic police squad and duty squad at three level networks, and adopt optical fiber, DDN and ISDN/PSTN and other communication means in accordance with the volume of business data..

Beijing : Road Condition Information Collection

Cisco.com

Inspect the loops, TV monitoring, microwave detection and frequency detection

1400 ring-shaped loop detector are set at 240 road crosses in Beijing for inspecting the vehicle flow and speed.

155 sets of microwave detection equipments are installed at the 2nd-ring and 3rd-ring road to detect the traffic flow data of 105 sections: flow, occupation rate, speed, travelling time and delay.

More than 160 sets of TV monitoring systems are installed within the 4th –ring roads of Beijing for capturing real-time road conditions.

Once there are traffic congestion, accident, troubled vehicles, security incident and other accidents, the information can be communicated to the command center through five channels at least..

First, through traffic control signal system,

Second, through TV monitoring cameras;

Third, through microwave detector;

Fourth, through patrol police;

Fifth, through “122” traffic emergency phone reporting system.

Xiangfan City Public Security Traffic Command Center

Cisco.com

- **Traffic Command System**
- **Traffic TV Monitoring System**
- **Auto-image-capture System of Traffic Rules-breakings**
- **Traffic-lights Control System**
- **Traffic Guiding System**
- **Traffic Information Inquiry System**
- **Traffic Communication System**
- **Driver's IC Card Management System**

Wireless Interphone (350 MB)

Traffic Management Information System

Cisco.com

- **Detection System for Rules-breaking Activities**
- **Enforcement System (Enforcement Station)**
- **Annual Inspection System**
- **Parking System**
- **Off-site Penalty System**
- **Vehicle-related Affairs System (Vehicle Administration Office)**

Traffic Police

Cisco.com

- 1. On Duty Urban Highway Police**
- 2. Highway Patrolmen**
- 3. Traffic Accidents Police**
- 4. Police for Vehicle Management**

Highway Traffic Police

Cisco.com

Special Service, Special Traffic Management Service

Route Traffic Police

Field Traffic Police

Stationed Traffic Police

Highway Patrolmen

Cisco.com

**Highway patrol squadron/30Km, >10
members**

**Freeway Traffic police group/40-60Km, >40
members**

Traffic Signal Control Technologies

Cisco.com

Point control:

Timed control, induction-based signal control

Line control: Green wave control

Area control: Regional control, and coordinated network control

Traffic Management Technologies

Cisco.com

- **Radar speed-meter:**
 - Radar speed measuring & photographing system
 - Portable radar gun for speed measuring
- **Alcohol detection**
- **Red light photographing: e-police**
- **Vehicle automatic monitoring system**
 - Speeding vehicles
 - Vehicles passing through key sections of road
- **Distance measuring & photographing at the scene of traffic accidents**

Video-based Traffic Monitoring

Cisco.com

Analog
Digital

**Professional video quality: 3M, 25-frame, 720*576
(big screen)**

**Desktop video quality: 1.5M, 25-frame, 720*288
(Video-on-Demand for internal staff)**

Police's Law Enforcement Information

Cisco.com

1. Investigation work information
2. Security work information
3. Border control work information
4. Security management information
5. City security information
6. Grass-root PS organization's information
7. Pre-interrogation & custody work information
8. Firefighting supervision work information
9. PS publicity work information
10. PS industry information
11. Information on the development of the leadership team
12. Information on PS science and technology research
13. Information on IT research
14. Information on PS education
15. Information on security work status
16. Other information

Border Check, Customs, Special Check

Cisco.com

“Border check”: Entry & exit border check

The ports opened up to the outside, such as the harbors, air ports, stations, and border passages

Border check authorities located in the opened up ports (known as “the frontline” for short)

Main task is to “manage people”, to check the passports, IDs, and visas of people entering or leaving the Chinese border; to monitor & protect the transportation tools; and to check the transportation tools & luggage if necessary

Specific work is managed by different border check stations.

Border check police and border control military officers

“Customs”: “Managing materials”, the offices of the General Administration of Customs in each opened up port

Border brigades, border check stations, border workstations, and **border police stations**

Border check & customs operate together in the same ports; when there is a border check station, there is a customs office; and vice versa

“Special check”: Check in special economic zones

The administration line of special economic zones (known as the “second line” for short)

“Border Pass of the People’s Republic of China” (or “Border Pass” for short)

The specific operations are the duties of the check stations of special economic zones (the check station of the Shenzhen Special Economic Zone and the check station of the Zhuhai Special Economic Zone).

“Shenzhen Entry & Exit Border Check Station”, manages eight entry & exit border check sub-stations at Luohu, Huanggang, Shekou, Wenjindou, Airport, Shatoujiao, and Sungang respectively, reports to the Entry & Exit Administration Bureau of the Ministry of Public Security, and all the staff members are professional police officers.

But the check station of the Shenzhen Special Economic Zone still remains part of the armed police system, and is still under the leadership of the Border Control Bureau of the Guangdong Provincial Public Security Bureau

The border check officers in Shenzhen wear the uniform of Public Security, but the special check officers in Shenzhen wear the uniform of the armed police

Criminal Investigation Technologies

Cisco.com

- Trace inspection: fingerprints, footprints, traces of tools, and traces of guns & bullets
- Document inspection
- Micro-material evidences
- Forensics
- Toxics & narcotics inspection
- Criminal imaging technologies
- Audio & video inspection
- Police dogs
- Criminal intelligence
- Identification & prevention of computer crimes
- Judicial expert testimony of mental disorders
- Judicial accounting & testimony
- Others: Psychological test, and mesmerizing technologies

“Networked” Prisons & Jails

Cisco.com

Aug 15, 2002

The Supreme People's Procuratorate, the Ministry of Public Security, the Justice Department held the National network-based management and dynamic monitoring on-site conference

Currently, the efforts to realize network-based management and real-time monitoring of prisons & jails are going forward in full steam in Beijing, Zhejiang, Heilongjiang, and Jiangsu.

By connecting with the information system networks of the prisons & jails, the procuratorate authorities can realize the real-time and dynamic 24 X 7 supervision each day, and can find out the detention period of a particular inmate in advance through the system, so as to remind police officers in charge to prevent and remedy cases of over detention

The practice of network-based management and dynamic monitoring will be gradually adopted by prisons and jails in different level around the country, in an effort to realize network-based management and monitoring of prisons & jails across the country in the shortest time possible.

“Networked” Prisons & Jails

Cisco.com

When a suspect is transferred to a jail, his/her information will be transferred to the management information system of the jail in real time from the computer system of the criminal investigation authority. The officer in charge can enter the ID number of the suspect into the system, which will extract the personal information and case information of the suspect from the population information system and the criminal investigation information system automatically, and compare the information with the Ministry of Public Security’s database of criminals on the run; if the suspect is such a criminal on the run, the system will give out an alarm.

The suspect will be transferred to the transitional jail room, and various activities of him/her will be tracked and recorded dynamically through the management information system of the jail.

After the conclusion of the criminal investigation stage, if the suspect is to be released without being convicted, the system will automatically transfer the case information to the local police station of the area where the suspect resides. Thus, a close loop is formed from the point the suspect enters the jail to the point he/she leaves the jail. The case information is transmitted automatically on the network in real time, the legal documents are printed automatically, and the information is updated and saved automatically, to form a complete and standard information flow.

Management of Migrant Population

Cisco.com

- **People involved in criminal activities in Beijing: over 60% are migrant population**
- **Hotels, guesthouses, and rented houses**

National Conference of Leaders in Charge of Prisons & Jails from Provincial PS Bureaus

Cisco.com

Bai, Jingfu
August 15

Prison & Jail Management Information System

Strive to realize network-based management of prisons and jails across the country in two to three years

Realize the sharing of information on inmates across regions and among different types of police