Cisco's Customization of China's Golden Shield to Suppress Falun Gong

Peter Li, Ph.D.

December 18, 2013

"The deeds were monstrous, but the doer…
was quite ordinary, commonplace,
and neither demonic nor monstrous."

Hannah Arendt, Eichmann in Jerusalem

Table of Contents

INTRODUCTION

This report looks at the role of Cisco Systems, Inc. in China and, more particularly, its customization of the "Golden Shield" network to enable Chinese security forces to monitor, surveil, and persecute dissidents in China, particularly Falun Gong believers. As shown below, this U.S. company has played a vital role in furthering and intensifying one of the Chinese Communist Party's most brutal modern repression campaigns.

China's "Golden Shield" system is "a massive, ubiquitous architecture of surveillance," largely set up and implemented around the turn of the 21st century.[1] Cisco was involved with this project even before its public unveiling, and took the lead role in its development. In its design and management of the extremely complex Golden Shield security system, Cisco has become gravely complicit in the targeted repression of Chinese victims of human rights abuse.

The design of the Golden Shield required detailed, integrated efforts by extremely specialized experts. The Cisco teams carrying out this work were based in San Jose. In reading the analysis that follows, it is important to ask two questions: 1) Why were American technology professionals, at the pinnacle of their profession, offering to create a network "solution" geared towards the commission of human rights violations including summary detention and torture?; and 2) regardless of their motives, did they in fact manage to accomplish this challenging technological feat?

***

[1] Greg Walton, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN CHINA, International Centre for Human Rights and Democratic Development (2001).

The answer to the first question is profit. Cisco's gained and maintained a stronghold in the Chinese technology market through its support of the Chinese Communist Party's suppression of Falun Gong through a massive political *douzheng*.

This term, which has played a pivotal role in the launching of Stalinist-style violent purges in China since the early days of the Party's rule, is used by high ranking leaders to identify a group or individual to be eliminated as an enemy of the Party. Such elimination is carried out through killing, physical incapacitation, or forced conversion (Mandarin: *zhuanhua*). Successful forced conversion constitutes the coerced repudiation of one's deeply held beliefs, the moral choices that determine one's character, and more generally, one's personal identify. This is the ideal/desired outcome for any *douzheng* campaign.

Because of the extreme practical and political ramifications of the *douzheng* process, the term's use is itself a major decision for Chinese Communist Party leaders. As is clear to anyone familiar with Chinese Communist Party policies and methods of social control, use of the term "*douzheng*" to define the Party's goals for Falun Gong was a clear statement of intent to wipe out the religion and its adherents.

Cisco's use of this term is profoundly disturbing. In internal documents describing its goals for the Golden Shield project, Cisco explicitly describes the purpose of the Golden Shield as the *douzheng* of Falun Gong (and other hostile elements). In the very same internal file, the company goes on to describe the persecutory purpose of the apparatus as a profitable "business opportunity."

***

The answer to the second question is yes. Cisco provided Chinese security forces with a full arsenal of features to accomplish the essential goals of the *douzheng* crackdown:

- **Identification (including invasive surveillance, tracking and monitoring)**
- **Apprehension and Isolation**
- **Forced Conversion**
- **Continued subjection to lifelong ostracism and continued surveillance, detention, or death**

The following is a step-by-step analysis of the most important design features and functionalities of the Golden Shield, based on GIFC's review of documents and insider accounts over the course of the past decade. The features analyzed below were all customized in order to facilitate, in the most effective way possible, the *douzheng* objectives listed above and in particular the forced conversion or *zhuanhua* of Falun Gong adherents.

I. ORWELLIAN SURVEILLANCE

Surveillance of Falun Gong believers is required to accomplish the various forms of human rights abuse constituting the *douzheng* campaign against them. In order to accomplish this, Cisco custom-designed intrusive Orwellian systems, as set forth below.

Signatures – Hunting Down Targets Based on Their "Digital DNA"

Unlike other dissident groups that can be identified by physical or linguistic indicia, Falun Gong posed unique challenges for those seeking to hunt them down in order to forcibly convert and suppress them. Since Falun Gong adherents are indistinguishable from the majority population except for their religious beliefs and/or related speech or activities, most of which occurs on the Internet, Cisco incorporated features into the omnipresent surveillance system in order to meet this challenge.

Cisco created a new, extremely potent tool: A dynamic, ever-expanding library of unique Falun Gong "signatures" which encode highly detailed models/archetypes of all potential Falun Gong Internet activity—i.e. recognition patterns with millions of variable factors (such as image components, words, and other electronic data)—that mark and catalogue all forms of Falun Gong Internet activity allowing instant identification and reporting.

These signatures serve as the basic library of Falun Gong data, which is used by various security features of the Golden Shield to identify Internet users as Falun Gong. For example, if someone sends an email in China which happens to contain an image of a person meditating in a Falun Gong lotus position, or contains a Falun Gong-related phrase or term, the Golden Shield alerts Chinese security forces to facilitate the tracking down and capture of the person sending whatever content matched one of the signatures.

Pervasive, Real Time Stalking Systems

Cisco created several customized "security systems" based in its specialized network devices, which update the Golden Shield databases to include the Falun Gong Internet activity, via the signatures above as well as other means of

detection. These systems include: "Log/Alert", "IDS/IPS", "Cisco Pix", and "IronPort," which provides real time notice to Chinese security tasked with the capture and suppression of Falun Gong.

Overarching Internet Surveillance System

Unlike most other countries where the Internet is decentralized and inter-connected via a large number of networks, the Chinese Internet is centrally managed and connected to the global World Wide Web via a few international gateways to ensure Party control. In other words, the Chinese Internet more closely resembles an Intranet: an internally connected network of computers.

At the heart of the Chinese Internet is the Internet Surveillance system. With one of its major goals to *douzheng* Falun Gong, this system operates as the "eyes and ears" of the Orwellian surveillance network. Using Cisco's custom-designed "digital DNA" identification tools, i.e. signatures, the Internet Surveillance System comprehensively monitors all Chinese Internet activity as well as traffic going across international gateways, scouting for any signs of Falun Gong activity. Once detected, the activity is immediately logged, transmitted and reported to the Golden Shield network; once identified as Falun Gong-related, any digital activity will be compiled and stored in the Golden Shield database. Moreover, one's online "address", name, and computer will be immediately blacklisted and subjected to heightened surveillance.

Cisco designed the Internet Surveillance system to carry out surveillance at an unprecedented scale, across all forms of digital communications. According to a Cisco marketer, Chinese police could remotely access all of a targeted dissident's online activity including surfing histories, email accounts and other online communications. Not only does this provide Chinese security agents wide-ranging access to one's family, employment and financial information, it also

allowed Chinese security to develop highly customized means of extracting information through threats and torture (*see* §III – *Zhuanhua*, *infra*). Indeed, once targeted, no online activity is beyond the reach of the "eyes and ears" of Big Brother.

Repressive, Falun Gong-specific Software Applications

Equally important to the anti-Falun Gong system functionalities described above, Cisco also custom-designed the Golden Shield's user applications to better facilitate human rights abuses against targeted adherents.

Applications custom-created by Cisco include, but are not limited to, the Falun Gong Web Announcement Server and the National Falun Gong Key Personnel Information System, which allows instantaneous identification and communication regarding any detected Falun Gong activity. Each of these was developed by Cisco as a customized software access point closely integrated with the hardware and network systems described above. Chinese security forces use these applications to locate specific Falun Gong adherents, or to seek out the locations and details of any recent Falun Gong presence or activity, electronic or physical.

War Room Applications

Cisco customized war room terminals and oversaw the design and integration of all other devices used by Chinese security to monitor the behavior of the entire Chinese population. Cisco customized the "War Room" command and control centers by which local Chinese security force detachments oversee and manage identification and further handling of Falun Gong adherents. All such interfaces are customized for incorporation into the structure of the Internet surveillance system.

Falun Gong-Driven Features

The Golden Shield as a whole was custom-designed to feature a multi-tiered design by which individual components (*supra*) detecting Falun Gong activity at any point in China could instantly communicate with each other and with Chinese security users at any other point in China—allowing instant coordination of the monitoring, tracking, and pursuit of the identified Falun Gong adherent. The system as a whole was also given a uniquely high hardware scale, capacity, and complexity in order to accommodate the unique demands of nationwide repression against the population of tens of millions of Falun Gong adherents. No local engineers/programmers had sufficiently relevant expertise to conduct such training; nor could anyone but the team designing the systems adequately design their training program.

II. APPREHENSION AND ISOLATION

Falun Gong Databases – A Directory of Intended Repression Targets

Cisco created and serviced database systems (building off of the custom designed "information gathering platform", described *supra* at page 3 and *infra* at page 9) containing information indispensable for apprehension and detention, such as but not limited to records of all previous encounters with Chinese security forces, physical location, "*hukou*" (city registration system) status, recent physical and online locations of any Internet access, physical characteristics of the person to be apprehended, potential ability to flee or otherwise evade capture, and finally a wide range of other data regarding work and social life that would aid in tracking the adherent to a place where it would be easy to capture him or her, etc.

The Falun Gong databases were custom-built into all of the core functions of the Golden Shield in order to ensure smooth and instantaneous coordination of apprehension and detention of any targeted Falun Gong adherent. Cisco also integrated its Falun Gong database infrastructure with the Golden Shield's full range of video surveillance features, the command and control center, and mobile police technologies. The databases were also made accessible through the Golden Shield network in Reeducation Through Labor camps, unofficial detention centers, psychiatric hospitals (used to lock up dissidents), so-called "black jails", etc. allowing for dynamic management of Falun Gong detainees in these facilities.

Falun Gong-Specific Applications

As noted *supra* at page 5, applications including the Falun Gong Web Announcement Server and the National Falun Gong Key Personnel Information System allow Chinese security forces to quickly and readily access information stored in the databases above, in order to identify targets of arrest, coordinate large-scale arrests by officers across jurisdictions, and ensure that any escaped Falun Gong adherent, or any released adherent seen as at risk of recidivism into their private religious practice of Falun Gong, can once again by apprehended and detained, etc.

Strategic Target and Attack Center

Cisco's customized control terminals and user interface, described above, were custom-integrated with the Falun Gong databases allowing Chinese security force personnel in "War Room"-like command and control centers to create highly individualized plans of attack to track, pursue, apprehend, and detain all identified Falun Gong adherents. Personnel overseeing all aspects of local

implementation of the crackdown on Falun Gong were able to simultaneously manage many cases and coordinate choices of specific adherents to apprehend and detain to maximize intimidation to the local Falun Gong community as well as to maximally deter local Falun Gong activity.

III. *ZHUANHUA* – FORCED CONVERSION

1. Golden Shield Torture/Forced Conversion Programs

The ideological conversion of Falun Gong practitioners was effectuated via individualized conversion programs created by special Chinese security units based on targets' individual susceptibility to various transformation tactics. These strategies were tailor made for each Falun Gong adherent and facilitated by Cisco's customization of the Golden Shield, as outlined below:

Thought Control

Thought control platforms made it possible for Chinese security to instantly access and automatically compile data from the various, scattered networks and data terminals comprising any and all sorts of information that might be relevant to the end goal of intimidating and coercing individual detained Falun Gong adherents to abandon their religious beliefs and begin to condemn the religion. This data—e.*g*., personal and family information, close associates, employment records, financial assets, and political views—allows Chinese security agents to build complete lifetime profiles of Falun Gong practitioners across China in order to develop highly effective individualized conversion techniques (i.e. craft highly personalized forms of threats, abuse, psychological pressure, physical and mental torture) based on individual susceptibility to various forced conversion measures. Some of the prevalent tactics include threatening to target close

friends or family members if adherents did not succumb to forced conversion. Each detainee's reactions to such treatment were also recorded and made instantaneously available to Chinese security forces for review, analysis, and further strategizing to achieve successful forced conversion.

The solutions designed by Cisco combine various sources of information seamlessly in a "webbed" (interconnected, cross-referencing, multi-tiered) architecture, where Falun Gong-related sensitive information is not only securely encrypted but also designed to be routed through the Golden Shield network and stored in the Falun Gong databases after a process of careful verification, inspection and cross-checking. These databases are themselves highly customized in order to maintain top-level secrecy and controlled access regarding Chinese security forces' torture practices against Falun Gong adherents.

All relevant Golden Shield features, including the "information gathering platform" described *supra*, were specially integrated with divisions of the Chinese security forces devoted solely or primarily to anti-Falun Gong operations, including forced conversion practices. These include the extralegal 610 Office (which oversees all aspects of the suppression of Falun Gong and especially forced conversion torture practices), the Political and Legal Affairs Committee (the Party security force division which reports to Party authorities as to the successful implementation of the suppression of Falun Gong and transmits higher-level Party orders), et al. The integration of the "information gathering platform" and other Golden Shield features with these specifically anti-Falun Gong entities allows the system to collect the information most relevant to forced conversion practices, as noted above, such as a record of previous subjection and reactions to forced conversion torture practices, assessment of ideological beliefs and psychological fragility, assessment of susceptibility to forced conversion, and other relevant data.

2. Sites of Torture

Cisco created and optimized a sophisticated "webbed" (interconnected, cross-referencing, multi-tiered) architecture and other structural features, customized to provide access to the Golden Shield's forced conversion functionalities to Chinese security agents implementing ideological conversion at various torture sites across China.

Cisco custom-designed the Golden Shield to ensure the instantaneous access of all necessary data to Chinese security forces tasked with the forced conversion of Falun Gong adherents. This was made possible by customizing the data provided via the Golden Shield to Reeducation Through Labor camps, detention centers, psychiatric hospitals, rehabilitation clinics, black jails, "love and care" centers, etc. providing access to the above information necessary to successfully carry out forced conversion via physical and mental torture. The custom-designed access points for Chinese security forces in such facilities also allowed security agents to update the databases to identify further points of vulnerability and ensure consistent, relentless intensification of the torture process for as long as necessary.

To ensure the confidentiality of sensitive Falun Gong information, access to these databases and information systems is further restricted only to special security agents, restricted members of the extralegal PLA, and agents of the extralegal 610 Office. This was particularly crucial as there is substantial opposition within the Chinese Communist Party and the security force hierarchy to the brutal torture practices used against Falun Gong adherents—secrecy of such practices is a key strategy used by the Party faction overseeing their implementation, in the attempt to avoid widespread knowledge of such abuses. Cisco designed the Golden Shield with this concern in mind.

3. Lifetime Surveillance and Torture

Cisco carried out the further comprehensive integration of the database systems above to enable the "dynamic" management of millions of Falun Gong adherents nationwide according to their level of susceptibility to forced conversion, with recidivistic practitioners often subject to increasingly severe further mental torture sessions. This integration also allows Chinese security to analyze, research and categorize various forms of transformation strategies for future deployment.

The Golden Shield's "lifetime" profile system ensures that, once targeted, Falun Gong adherents never escape the attention of Chinese security forces. Those who persist in their religious practice (i.e. are not successfully "transformed"/forcibly converted) are subjected to continued harassment and abuse. Those who fail to transform can be dispatched to ever more violent torture, either in the same facilities or, e.g., by being sent to psychiatric facilities to be drugged. In other cases, those who fail to be transformed die during the torture process. At minimum, anyone who enters the Golden Shield databases faces the high likelihood of the above outcomes.

To ensure the effectiveness of the apparatus, Cisco tested and verified all of the above features to ensure that it fulfilled the Golden Shield's persecutory purposes. Cisco further trained all relevant members of the Chinese security forces in the details of how to use the above systems, features, and applications. Cisco also had to devise this training process—all the more so because this technology was previously unknown and unavailable in China, and no local engineers/programmers had sufficient relevant expertise to conduct such training; nor could anyone but the team designing the systems adequately design their training program.

IV. CONCLUSION

The Chinese Communist Party appears to be entering into a period of reform. Important measures currently underway include the abolition of the Reeducation Through Labor system and efforts to eliminate the use of torture in obtaining forced confessions. Perhaps the Golden Shield, too, will one day become a thing of the past. But we are still left with the question, how does a person or a corporation (run by people) come to place profit or personal gain above the rights of all persons to dignity and a life free from torture?