

Beijing's Rising Hacker Stars... How Does Mother China React?

By Scott Henderson

Editorial Abstract: Mr. Henderson examines a major hacker organization in the People's Republic of China, exploring the linkages between government and private network exploitation. He reviews political, military, and economic targets, and warns against using a Western model to explain intricate online behaviors and motivations.

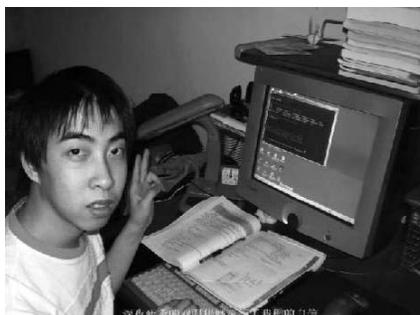
In 2007, government information systems inside the US, UK, Germany, France, Japan and Taiwan fell victim to cyber attacks. While not conclusive, most indicators pointed to China as the country of origin and the possible culprit. Based on growing online demographics, it is very likely we will see an increase in Chinese hacker activities in the coming year. Security experts at Arbor Networks even predicted this year (2008) would be the "Year of the Chinese hacker."

While little is known about military hackers employed by the Chinese People's Liberation Army, we are starting to get an understanding of their civilian counterpart known as the Red Hacker Alliance. This organization, responsible for many of the headline grabbing accounts of "Chinese hacker attacks," was formed in response to the 1998 ethnic riots in Jakarta, Indonesia. The Indonesian populace unfairly blamed their ethnic Chinese community for the country's out of control inflation. Indonesian citizens turned on the Chinese living among them, committing murders, rapes, and destruction of businesses. News of these atrocities filtered back to individual Chinese hackers, who in retaliation formed the "Chinese Hacker Emergency Conference Center," sending e-mail bombs to Indonesian government websites and mailboxes and conducting Denial-of-Service (DoS) attacks against Indonesian domestic sites.

Since their founding, the group has been involved in at least five major cyber conflicts. Its membership has climbed from a few thousand to around 300,000—many of whom are young nationalist males in their early to mid-20s. Initially composed of only seven rudimentary websites, the alliance now contains 250+ stations stretches across three major municipalities; seventeen

provinces; one autonomous region; and the Special Administrative Region of Hong Kong.

For network security personnel throughout the world, determining the government affiliation of the Red Hacker Alliance has become a key question demanding an answer. Are they, or are they not, an officially sanctioned apparatus of the state in terms of tasking, oversight, and control of the organization? The simple answer is *no*. They are not a branch of the government



Chinese hacker "Withered Rose" greets his online community. (thedarkvisitor.com)

or the military. Chinese hackers are most likely who and what they claim to be: an independent confederation of patriotic youth dedicated to defending China against perceived threats to national dignity. However, it is also true the question of direct government affiliation is itself flawed, and the simple answer of "no" is highly misleading.

The central problem with our inquiry is that we are viewing the situation from a US paradigm and applying our cultural bias. In China, independence from government direction and control does not carry with it the idea of separation from the state. The PRC government views its citizenry as an integral part of Comprehensive National Power, and a vital component of national security.

The State and Alliance Relationship

The masses figure heavily into China's strategic calculations and will be actively used in times of conflict and peace. So, while applying the label of a nongovernmental entity to the Red Hacker Alliance is true, it is also deceiving. Affixing this tag implies the alliance is not associated with the official intelligence structure in any capacity. This is also incorrect. The inability to derive a "yes" or "no" answer to this problem is rooted in our tendency to apply mirror imaging of US societal norms—where they do not exist.

From a Western perspective, the idea of active espionage against another nation requires government initiative, involvement, and direction. It is hard for us to conceive of links being formed between state authorities and quasi-freelance intelligence operations, simply because it does not fit our preconceived notion of the proper relationship. There is a very good chance this is exactly the type of association taking place between the PRC central government and the Red Hacker Alliance. Western nations assign virtually no intelligence-gathering role of any kind to non-governmental citizens in peacetime; even during periods of active conflict, Western citizens are probably best defined as "heightened citizen watch groups." China on the other hand, does not make a distinction between these two responsibilities; citizens are expected to take part in both arenas. The People's Liberation Army emphasizes the integration of military and civilian roles in their strategic doctrine of future wars:

In the high-tech local war which we will face in the future, the role of the masses as the main body of the war is embodied by the country. The great

power of the people's war is released through comprehensive national power, the combination of peace time and war time, the combinations of the military and the civilian, and the combination of war actions and non-war actions. Besides the direct participation and cooperation with the army's operations in the region where war happens, the masses will support the war mainly by political, economic, technical, cultural and moral means.

The Chinese believe in the idea of a *People's War*, in which the entire population is mobilized to struggle on behalf of the nation. The Red Hacker Alliance will gladly assume its role as protector and seek out targets of opportunity to attack. Being a civilian organization will in no way limit their participation in striking out at the enemies of China. If history is any indication, as the numerous examples of Chinese hacker attacks represent, they will take the lead in launching preemptive or retaliatory assaults.

So, what would this quasi-official relationship look like and what are its characteristics? An interview with a Chinese hacker from Beijing provides an excellent example of this "nontraditional" relationship:

"One Beijing hacker says two Chinese officials approached him a couple of years ago requesting 'help in obtaining classified information' from foreign governments. He says he refused the 'assignment,' but admits he perused a top US general's personal documents once while scanning for weaknesses in Pentagon information systems 'for fun.' The hacker, who requested anonymity to avoid detection, acknowledges that Chinese companies now hire people like him to conduct industrial espionage. 'It used to be that hackers wouldn't do that because we all had a sense of social responsibility,' says the well-groomed thirty something, 'but now people do anything for money.'"

This technique used above typifies the same soft-control the government exercises on human intelligence collectors in the US and other countries. China relies on a broad informal network of students, tourists, teachers, and

foreign workers inside targeted nations, collecting small bits of information to form a composite picture of the environment. Rather than set a targeted goal for collection, they instead rely on sheer weight of information to form clear situational understanding. Alliance members make ideal candidates for flexible operations; they have proven themselves to be capable, patriotic, and motivated. To clarify, this is not to suggest that every member or even a majority of the members have connections with the government. In fact, there are probably only a select few who have any dealings whatsoever with officials.

Additionally, there are intricacies and complexities of this dynamic that move it far beyond the headline grabbing probes for international secrets. Political, economic, and social issues



*Chinese Trojan database.
(thedarkvisitor.com)*

account for a majority of the contacts between the two, and require a delicate balance of constraints and freedoms. We can even surmise that there are times when an uneasy truce exists between the two parties. Such unease stems from alliance concerns over a possible crackdown on the organization, and the government's fear of a hacker instigated rebellion among its youthful members. Better understanding points where mutual interests converge will aid us in unraveling what mechanisms bind them together, and how they might interact.

Intelligence and Economics

From the Party's viewpoint, the Red Hacker Alliance must have benefits that outweigh their liabilities. If political activism and attempts to penetrate foreign systems brought about only international condemnation and created points of contention between

China and other nations, the Party would halt the Alliance's activities. Beijing is well aware of the possible downside this group represents, and the inherent dangers of their involvement—especially during times of crisis. An international dilemma on the verge of resolution might be exasperated by cyber attacks on infrastructure or governmental institutions, possibly resulting in unforeseen and unmanageable consequences. On the other hand, if the returns are greater than the costs and the benefits outweigh the risks, then the government would see the Red Hacker Alliance as an asset—and allow them to continue. At the moment, there are no indicators that authorities in Beijing are making any attempts to rein in or shutdown the alliance, a telling sign that the cost-benefit analysis is still in the alliance's favor. So, what factors make it more profitable to protect the organization, and risk a possible escalation of international tensions, than to be rid of them?

The most obvious reason for Beijing's apparent tolerance of the Alliance is that it likely receives valuable information from the group. Thousands of hackers, working around the clock, could surely fill in some of the blanks of a composite intelligence picture. As a civilian organization, the Red Hacker Alliance also provides the government with plausible deniability. Even if Alliance members are caught red-handed breaking into a system, it is easily disavowed as the actions of overzealous youth, not that of the government. In December 2005, as accusations of China's involvement in government-sponsored hacking heated up, People's Republic of China Foreign Ministry spokesman Qin Gang flatly denied charges of PRC government involvement, asking the US to produce any information proving these allegations. The foreign minister offered nothing further, simply dismissing the idea in its entirety. Qin held fast to the argument that Chinese regulations prohibit attacks on the Internet, suggesting that should be proof enough they were not involved. Such an approach is highly effective at deterring further inquiry. It requires

the US reveal specific incidents and explain the techniques that led to those conclusions, thereby revealing US operational capabilities in intrusion detection, backtracking, and identifying attacking points of origin.

We should also be careful in assuming the relationship between the government and the alliance is a one-way street, with authorities requesting information and Red Hacker Alliance members providing it. It is quite possible there are times when the alliance, of its own volition, initiates collections against certain targets and then supplies such sensitive data to the government. Owing to the increased entrepreneurial nature of the organization, we cannot rule out financial compensation as a possible motivator for breaking into foreign systems. Going even further with this speculation, we cannot be certain the Chinese government is the only client or requestor for information. This knowledge is highly valuable to other governments, or even private companies around the world.

Corporate espionage is another arena where we must put aside our cultural bias and make judgments based on the Chinese system, rather than Western practices. If someone asks a US citizen “Who would be the most likely suspect in a crime involving the theft of corporate secrets for financial gain?” The US answer would probably be “another company.” That the government would condone or even encourage industrial spying and data theft for fiscal gain is a very remote idea for us. However, the Chinese government does not divorce itself from domestic industry—all assets inside China are viewed as assets of the state. Financial institutions are deemed a vital component for the health and stability of the nation, at least on par with if not on a higher priority, than development of military capabilities. Hacker efforts to assist in advancement of state enterprises, whether offered in return for monetary compensation or not, would be viewed as advantageous and likely “overlooked” by officials.

In a wave of industrial spying that began in August 2004 and lasted through at least the first quarter of 2005,

hackers from China unleashed the *Myfip Trojan* on corporate computers. Myfip is designed to search for files related to high-tech research and development, and send them back to an individual named Si Wen in Tianjin, China. Joseph Stewart, a senior security researcher and the man responsible for reverse engineering Myfip, noted Tianjin is China’s third-largest city and the second-biggest hub for manufacturing, particularly electronics. Notably, the attacks were so brazen, the hackers didn’t bother to obscure their location, a norm for most experienced hackers. Weighing in on the issue, Chief of iDefense John Watters said “Nothing suggests that Chinese authorities are vigilantly prosecuting those who are attacking foreign interests. They turn a blind eye to it as long as it doesn’t oppose national interests.”

Sectors where the financial interest of the Alliance and the security interests of the state coincide could present even greater difficulties for outside industries wanting to protect trade secrets. China’s rising energy needs and its worldwide search for energy resources present a prime example. There are tremendous pressures exerted on the state to sustain the country’s forward economic momentum, and to do so they must ensure a consistent and steady fuel supply. The competition to secure finite resources such as oil and natural gas can be highly competitive, and the methods to attain them may move far beyond those of traditional market mechanisms. Chinese hackers, working for personal gain, could find a lucrative market in the sale of information related to the petroleum industry. The state may be more inclined to turn a blind-eye to the practice, if it facilitates expansion of Chinese industrial interests.

Political

In addition to intelligence gathering and economic interests, politics are a driving force that binds the alliance and government together. The political front can be divided into two distinct categories: domestic and international. Internal or domestically-motivated political hacking is aimed at dissident elements and separatist movements

inside the country, extended to supporters of those same movements outside the country. Recipients of these attacks typically threaten national sovereignty and challenge the legitimacy of the ruling party: the Falun Gong; the Free Tibet movement; and Hong Kong activists.

In 2002, dissident groups outside of China complained Chinese hackers attempted to shut down their operations through virus and Trojan attacks focused on the e-mail addresses of the Falun Gong, banned news sites, freenet-china.org, and Xinjiang independence activists. Notably, the attacks began at roughly the same time the PRC Minister of Public Security called for more aggressive measures in going after foreign forces subverting China via the Internet. Chong Yiu-kwong, a human rights activist who organized democracy marches in Hong Kong, discovered that his e-mail was being monitored, noting:

I didn't know that my computer had been monitored ever since, until I found that all my e-mails from the account registered to the University of Hong Kong disappeared all of a sudden. I approached the computer center of Hong Kong University. They told me that my account had been monitored by three different IP addresses from China and that information from the account had been downloaded every few minutes.

A Chinese Internet security official described separatist activities as one of the major trends in cyber crime for 2002. According to this account, Falun Gong practitioners used the Internet to spread their philosophy and organize illegal activities. “Splittist” and anti-Chinese elements had evoked disunity and made attacks on the government and Party leadership. Luo Gan, a member of the Political Bureau and Secretary of the Central Commission on Politics and Law, identified cyber crimes as one of the three most important problems facing the country:

“Hostile forces at home and abroad as well as the Falun Gong cult are doing everything in their power to spread rumors and launch attacks on the Internet... Hostile forces and some people with ulterior motives may disrupt our Internet system through such means

as computer virus attacks and hacker attacks. Other illegal and criminal acts, such as online financial fraud, are also growing.”

In international disputes, Beijing has been able to count on the Red Hackers as a surrogate political hammer, and a rallying force for mainland solidarity. Historical accounts of the Alliance, from its inception to present day, demonstrate an organization that aggressively backs governmental policy through flexing cyber muscle. As documented in the book *The Dark Visitor*, these international cases include the attacks against the United States, the United Kingdom, Japan, and Indonesia. Other favorite targets are elections and referendums that touch on Taiwanese independence. During the June 2005 Asian-Pacific Economic Cooperation forum held in Seoul, an officer of the Taiwanese Criminal Investigation Bureau approached PRC delegates and requested their assistance in a joint crackdown on hacker attacks. Chinese delegates “cold-shouldered” the Taiwanese officer’s request.

Favorable public sentiment for the alliance’s nationalistic stances also provides some degree of guaranteed protection and support from the government. Ordinary citizens see them as a ‘voice for the people,’ stretching across great distances to right the wrongs against China. Some circles view famous Chinese hackers as Hollywood stars and not criminals. During the Sino-Japanese hacker attacks of 2000, Japanese officials requested that the websites of known hackers in the Guangxi, China area be shutdown for attacking Japanese websites. Police responded that they had no intentions of doing so, because it was a “patriotic” website.

Recruiting

China, which is still in the early stages of informationizing the nation and its military, recognizes the disparity in technical knowledge and experience between itself and other countries. To some extent, and in certain circles, the government has also come to appreciate this same gap between the older and younger generations. It is easy for us to lose sight of the fact that China has only

recently gained access to the Internet, and the migration process from social elites to the average citizen has taken some years. Familiarity and comfort levels with new programs—and the Web in general—are likely sharply divided between age groups. Chinese youth, like those in most nations, are more flexible and quickly adapt to new technologies while the older generation struggles to incorporate it. China’s elders are now reaching out to their children for help in understanding the uses of this new technology and the children are eager to assist.

Evidence taken from Chinese Internet forums and news broadcasts demonstrates that members of the Red Hacker Alliance would like to be a state-sponsored agency, and are somewhat offended they are not. In August 2005, *Phoenix Television News* carried a report that Chinese hackers wanted to be recruited by the government to form network security units in order to protect the safety of domestic networks. Postings on the *Honker Union* of China’s website were in firm agreement:

“We need to move toward standardized honker unions. We can’t wait until the nation has a crisis to act; we must be prepared to do something meaningful for the motherland. Why can’t we become a government-approved network technology security unit?”

According to other postings, various members of the organization had learned of foreign countries establishing “hacker network security units” and felt China should do the same, noting “It should have been this way earlier! The US, Westerners, Israel, and even the good guys have all formed hacker army groups! We can’t lag behind!”

Similarly, portions of the government have expressed interest in recruiting or at least learning from members of the Alliance. Following the Sino-US cyber conflict of 2001, ignited by the mid-air collision of a US reconnaissance aircraft and a PRC fighter aircraft, renowned Chinese military expert Professor Zhang Zhaozhong expounded on the vital significance of the 7-day network war. He suggested the government officially research these real-life network

warfare experiences for the benefit of the country. As the Director of the National Defense University’s Military Science and Technology and Equipment Research Department, Professor Zhang pointed out that during the course of the cyber conflict, Chinese hackers had developed many new tactics and gained much experience.

However, he also believed neither the Chinese nor the US government could tacitly condone this type of behavior, as it was harmful to the relationship between the two nations, being at odds with both national interests. Professor Zhang also expressed concern over the violation of treaties and laws. He felt that on the one hand the hackers should be commended for their well-intentioned spirit and motives for carrying out the attacks, but on the other they needed to be educated on the serious consequences of these attacks—and how easily innocents can be harmed.

Returning to his argument for studying this incident, Professor Zhang brought up President Clinton’s invitation for expert hackers to attend a meeting at the White House to discuss network security. Perhaps such an invitation could be used as a precedent for China to explore the “special role” of hackers. According to Zhang, network warfare was one of the measures of a state’s comprehensive national power. To underscore the importance of the study, he gave examples of the levels of difficulty in systems penetration:

“While it is relatively easy to tamper with a few Web pages, it is much harder to attack the Department of Defense’s network. Trying to penetrate the Pentagon, stealing nuclear secrets, or passing yourself off as a high ranking US military commander issuing orders to operational units is like reaching for the stars.”

Even though this mutual attraction toward collaborative efforts could be seen as a positive trend in the relationship, in the end it may produce the opposite effect. Such actions may wind up as a source of tension between the hackers and the Chinese government. In early 2006, members of the Red Hacker Alliance were dissatisfied with the government’s

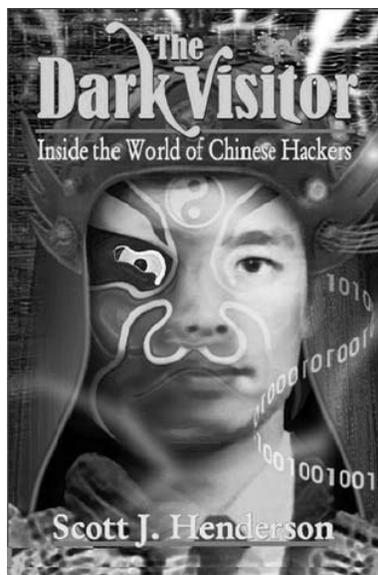
slow reaction in responding to what they considered a deterioration of the domestic network security environment. The Alliance began taking matters into their own hands. Through monitoring of foreign hacker websites, Chinese hackers had discovered numerous daily intrusions into Chinese government systems. The foreign hackers were making a game of counting the number of Chinese servers they could access. When alliance members attempted to notify officials of these security vulnerabilities, they were rebuffed, and told appropriate security firms were handling the situation. In some cases, it took days for the defaced websites to be discovered and returned to normal. The frustrated Chinese hackers, in an effort to reinforce their warnings of the defective security measures, took to defacing their own government websites. One hacker felt it might even have ramifications on any future cyber warfare with Japan:

If there really is a China-Japan Hacker War in the future, will this type of network technology do? Last week I spent an immense amount of energy to get into a petty Japanese trash website. I uploaded the modified main page. Half an hour later I took a look and its main page was, to my surprise, restored. Looking at those websites, those Chinese websites, which are, moreover, the websites of government departments, they were hacked over a week ago and still no one knows. Geez!

The weakness of government servers may be another possible explanation for cyber espionage charges leveled at China. Civilian hackers inside the country and foreign hackers outside the country, hijacking these systems, could account for a large number of the attacks originating from Chinese government owned resources. It is doubtful that the People's Liberation Army or any other affiliated group would attempt intrusions from accounts so easily identified. However, independents could find their servers easily co-opted targets and excellent launching pads for attacks. In March 2005, the Ministry of Public Security arrested a man from Hubei Province for forming a Botnet of 100,000 stolen computers.

According to the bureau, of the 100,000 infected, more than 60,000 were inside China, with a portion of those being government computers. A year later, Xinhua News Agency reported that in the first quarter of 2006, hackers had "changed information" on 2,027 official government websites. The 2006 first quarter statistics almost matched the total for all of 2005.

A further blurring of the lines between civilian and government ties is the way the Chinese Communist Party co-opts public use facilities, drafting them into military service. Western corporations may contract the government on issues of national



defense—but they are not "drafted." In 2003, Dongshan District of Guangzhou China, one of the major science and technology centers in the Southern region, spent US \$54,000 to turn the provincial telecommunications company, data communications bureau, microwave communications bureau, and Southern Satellite Telecommunications Services Corporation into a militia information warfare battalion. While these public facilities were becoming an official unit in the militia battalion, others such as NetEase Guangdong and the China Unicom Paging Company in Guangzhou were being brought onboard, even though they did not have an established mission. The Guangdong area has been cited as one of the major areas for "government sponsored" hacking, and activities of

groups such as these may be adding to the confusion of what is state-organized and what is civilian.

Communications

An interesting facet of the interaction between the government and the Red Hacker Alliance is the evolution in means of communications between the two. Without direct control over the daily workings of a group, how do you signal that they have crossed a line of departure, and it is time to cease certain activities? Again turning to the US-Sino cyber conflict of 2001 and anti-Japanese protests of 2005, a picture of "indirect communications" through mass media, universities, text-messaging, and online postings begins to emerge. The ability to ensure compliance with these directives seems tenuous at best, and may aim to keep the situation under control, rather than enforce 100% observance.

When authorities in Beijing decided the hacker war between China and the US had gone on long enough, they began issuing public statements, then contacted leaders of the alliance telling them that it was time to stop. The opening government salvos came from a variety of sources, all aimed at getting their message across?

- Official website of the *People's Daily*: "The attacks by the Honker Union of China, or Red Guests, on US websites are unforgivable acts violating the law. It is Web terrorism."

- Liao Hong, the director of the *People's Daily Online* editorial office:

"We understand the passion of these hackers but we do not endorse their way of expressing it. We do not want to offend patriotic Web surfers but it is important we alert the public to the risk of such acts and prevent further disasters."

- Officials from China's Internet security: "The war between Chinese and American hackers that led to the White House website being shut down was illegal."

- Spokeswoman for the Internet Safety Bureau, under the Public Security Ministry: "Such attacks are not legal. It is against the law to enter other people's systems."

- Su Zhiwu , Vice-president of the Beijing Broadcasting Institute: “Sino-US conflicts should be resolved through diplomatic channels, not hacking maneuvers.”

On 15 August 2001, primary Red Hacker Alliance leader Wan Tao announced a temporary termination of attacks on foreign/enemy websites. According to Wan, this was based on instructions from government departments. In May of 2002, after negotiating an agreement with five other Chinese hacker websites, to include the Honker Union of China, a joint statement called for an end to anniversary attacks recalling the 2001 incident.

From 2001 to 2005, the government gradually developed more sophisticated and expansive methods for communicating with its patriotic youth. Simple calls from recognized state newspapers and agencies were supplemented with Web postings and text messaging. The Party quickly grasped that traditional methods alone were inefficient at reaching a generation that felt more at home on the computer, and who used cell phones to communicate with their peers.

Beginning in April 2005, anti-Japanese demonstrations spread across China. Japan’s bid for a seat on the United Nations Security Council and additional revisions to history texts that downplayed Japanese actions in WWII brought out large crowds of Chinese protestors. The demonstrations, ranging across cities from Beijing to Shenzhen, were characterized by attacks on anything symbolic of Japan: government buildings, cars, businesses, and restaurants. There were even reports of Japanese citizens being attacked during the protests.

Toward late April, the Ministry of Public Security was tasked to halt the demonstrations. Using Internet postings and text messages in combination with traditional print media, the ministry ordered protestors not to organize anti-Japanese demonstrations without police approval. China’s Minister of State Council Information summed up the Party’s ability to control the populace:

“Most citizens obey no-demonstration orders... You need to

understand that Chinese citizens still respect the government. So if the government makes clear that this kind of demonstration is not OK, 90% of the people won’t go.”

Conclusions

The history of the Red Hacker Alliance clearly shows it to be a civilian initiated and run organization. The rapid growth from a few cells, to several hundred thousand members has been fueled by nationalism and international incidents. While there have been occasional sparks on both sides of the aisle, the Chinese government and the alliance have maintained what can be characterized as a status-quo relationship. Neither party is ready to embrace or reject one another. However, with the shift away from nationalism and simple website defacements to hacking for monetary gain, it is unlikely both sides can maintain this equilibrium.

Beijing faces several dilemmas in dealing with the Red Hacker Alliance. On the one hand, it is much better to have a large number of young males protesting foreign incidents outside the country than focusing their sights internally. The alliance can be useful in times of political conflict, and in the past it has been more of an annoyance to foreign governments than an outright threat to Chinese national security, infrastructure and economics. This has kept Beijing’s external pressures to a minimum.

Alternately, the days of simple annoyance appear to have past. Many

nations strongly protest the People’s Republic of China, asking them to reign in their civilian hackers—and the perception is growing they are a centrally-controlled entity. There is hardly a government, military or industry that has not been the subject of some sort of attempted intrusion by Chinese hackers. The patriotic aura has long worn off the Alliance, leaving much less sympathy in the Party leadership’s eyes.

Given these two sets of conflicting dynamics, Beijing will need to either disband the organization, or incorporate it into a more manageable state-directed enterprise. Disbanding the Alliance is unlikely, as such a move provides few benefits to the state and leaves behind a large number of disgruntled youth looking for an outlet. Incorporation provides a new security body for the country’s information systems and a method to curtail the worst of the group’s activities.

It is vital we accurately understand the unique relationship between the Chinese government, the Red Hacker Alliance and other hacker groups. This is only a preliminary step in grasping the complexities and intricacies that shape the movement. Without this knowledge, it will be difficult to anticipate the next wave of attacks or the motivations behind them. We must confront two equally difficult situations: we must understand if we face a state sponsored attack—or the act of a defiant child. 

