1. BACKGROUND

1.1 About TibCERT

The Tibetan Computer Emergency Readiness Team (TibCERT) is a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community, expanding Tibetans' technical research capacity on threats in the diaspora, surveillance, and censorship inside Tibet, and ultimately ensuring greater online freedom and security for Tibetan society as a whole.

1.2 Purpose

The purpose of the TibCERT quarterly bulletin is to share updates about TibCERT, advise on threats seen in the community, and report on issues inside Tibet related to cybersecurity.

1.3 TibCERT Updates

It has been almost a year since the Tibetan Computer Emergency Readiness Team (TibCERT) was launched. TibCERT's Digital Security Ambassadors are now located in four major Tibetan settlements, e.g., Dharamshala, Dehradun, Mundgod, and Bylakuppe. There are currently 41 stakeholders which include institutions, organizations, monasteries, and schools. TibCERT has drafted digital security policies with most of the members, as well as conducting digital security trainings and incident responses for both digital security and technical issues. We have also implemented endpoint security tools for a few of the stakeholders and are planning to implement them with other members as well.

1.4 Summary

This second issue of the TibCERT quarterly bulletin includes:

1. A report on Whatsapp attacks from fake Whatsapp personas which occurred from November 2018 to May 2019. Many senior staff from various Tibet human rights organizations received Whatsapp messages with links containing a one-click exploit for their smartphones (both iOS and Android). In this report, we also mention solutions to avoid becoming a victim to such attacks.
2. Changes in technology for Tibet, such as:
   a. Development of a new system of surveillance called "Gait recognition." This program system identifies a person by taking their silhouette from a video and analyzing the way they move, even if the silhouette is as far as 50 meters away.
   b. Implementation of a "Social Credit System" which can be used as a system to control the behavior of Tibetans online, leading to greater self-censorship and restrictions.
   c. Development in speech and speaker recognition by an artificial intelligence company to monitor minority groups such as Tibetans and Uyghurs.
3. Technology issues in China, such as:
   a. Chinese tech giant Huawei's many controversies involving the United States which have greatly affected Huawei. For example, Google is barred from selling Android licenses to Huawei phones, resulting in Huawei phone users not having access to Google apps like the Google Play Store.
   b. Censorship and the banning of certain apps from the Chinese iOS App Store.
   c. Stopping the streaming of NBA preseason basketball games by China in response to an NBA executive's support of the Hong Kong protests.
   d. A Waterhole attack targeted at minority groups, particularly the Uyghur population. Attackers found various vulnerabilities to iPhones, thereby compromising phones instantly just by visiting an infected website.
   e. A new Chinese government policy that requires facial-recognition when buying a SIM card. This policy goes into effect in December. The Chinese government claims that this policy will keep the rights and interests of cyberspace safe for citizens.

2. DIGITAL SECURITY UPDATES

2.1 Whatsapp Report

TibCERT and the Citizen Lab published a report on a one-click mobile exploit targeting Tibetans. Last year, in the early hours of November 13, 2018, a senior staff member at a Tibetan human rights group was contacted on Whatsapp by a previously unknown number. The sender claimed to be "Jason Wu," head of the "Refugee Group" at Amnesty International's Hong Kong branch. "Jason Wu" tried to present as a credible person by mentioning social media reports on a recent self-immolation. During the conversation, he sent links to information he claimed to be related to the case, wanting to verify for use in an Amnesty International report on human rights in China, as well as for an upcoming statement critical of the Chinese government's treatment of ethnic minorities. While such a request is common for activists in the Tibet movement, this request had sinister motives behind it. "Jason Wu" is a fake person and the links contained exploits (malicious code that takes advantage of software vulnerabilities) for iOS. This exploit works on iPhones running a vulnerable version of iOS (11.0 through 11.4). By clicking the link, the iPhone would be infected with spyware, stealing data from the device and apps running on it.

The Citizen Lab of the University of Toronto reports that this campaign is the first documented case of one-click mobile exploits used against Tibetans, reflecting an escalation in the sophistication of digital espionage threats targeting the Tibetan community. This campaign appears to be carried out by a single operator that the Citizen Lab called POISON CARP.

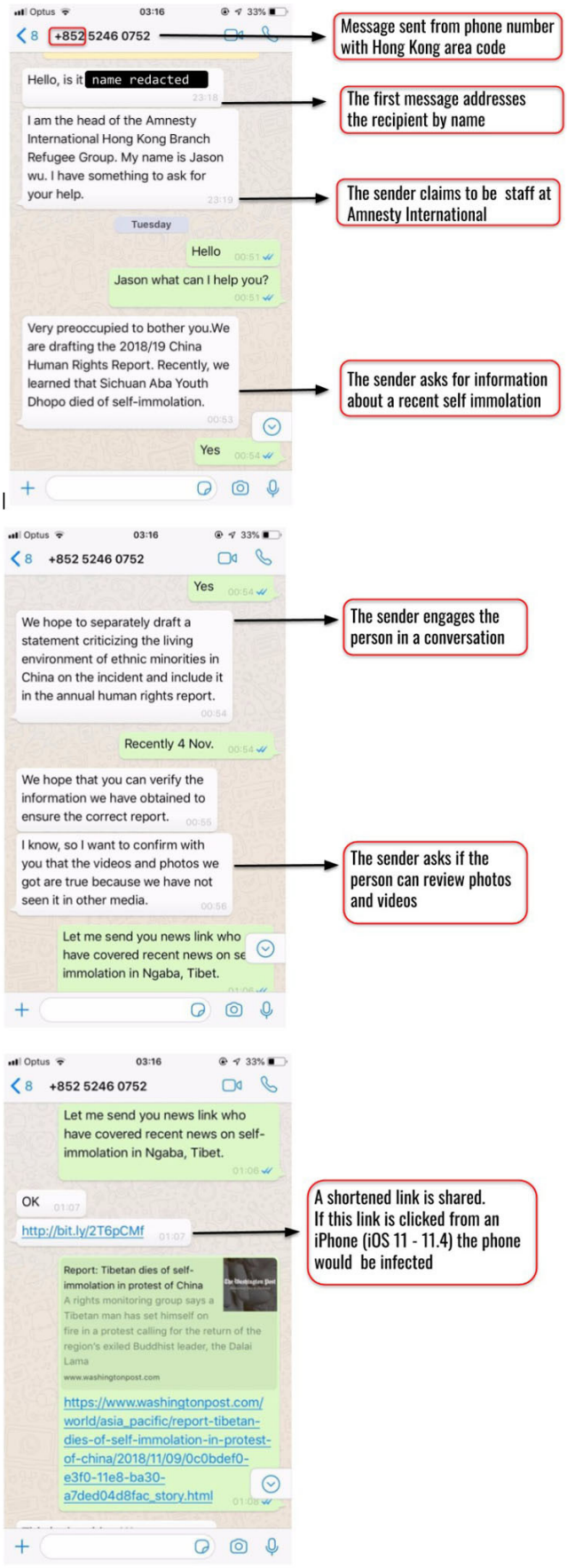


Figure 1: An infection attempt in the early hours of November 13, 2018 shows the level of effort put into social engineering.

The Infection Attempts

In addition to targeting iPhones, the spying campaign also targeted Android devices and tried to use malicious Open Authentication (OAuth) applications to gain access to Gmail accounts. Over the course of the campaign, the Citizen Lab collected one iOS exploit and eight distinct Android exploits. In total, 15 attempts were made to infect mobile phones.

Of these 15 infection attempts, 12 were sent to Tibetan targets with links to the iOS exploit. All but one of the attempts were sent between November 11-14, 2018, with the last attempt sent on April 22, 2019. Table 1 shows the targets and exploits sent to both Android and iOS phones.

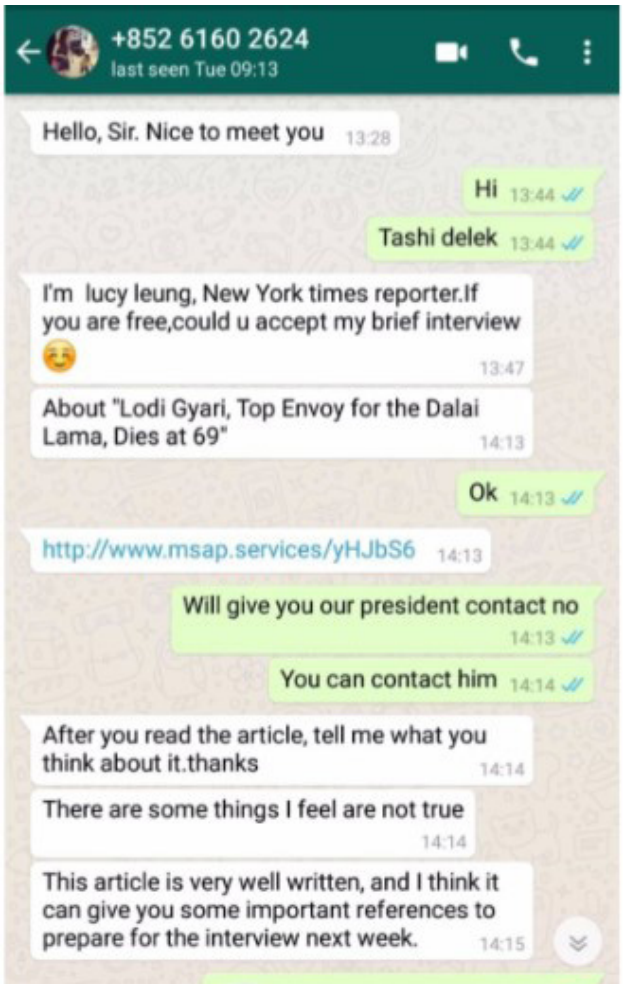
	iOS	Android
Exploit(s)	1	8
Targets	12	3

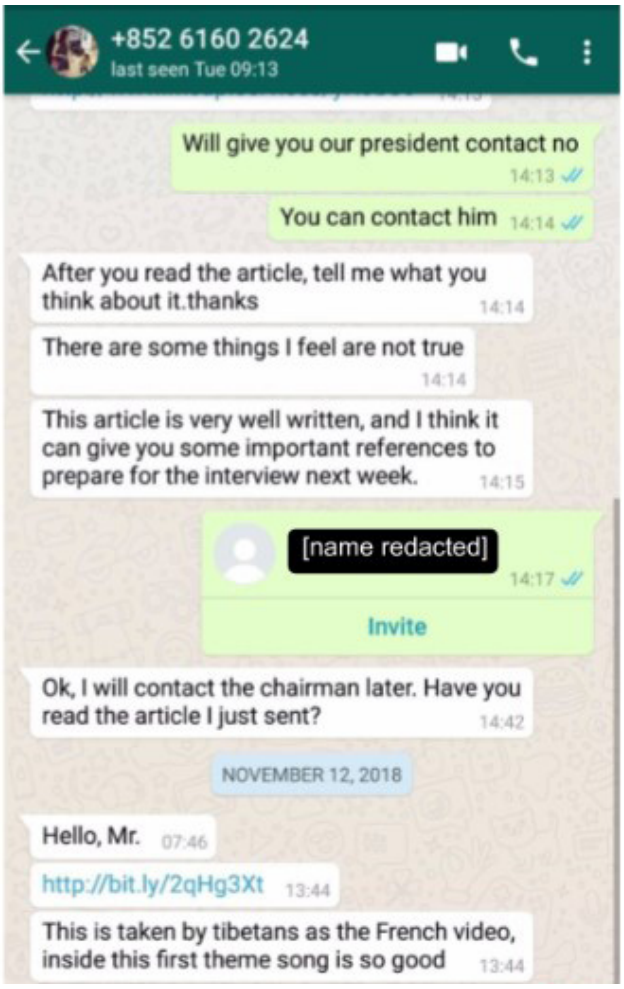
Table 1: Infection attempts across iOS and Android phones.

The targeted individuals received malicious links in individually tailored WhatsApp text exchanges from seven fake personas designed to appear as journalists, staff at international advocacy organisations, volunteers to Tibetan human rights groups, and tourists to India. The fake personas actively engaged in conversations and persistently attempted to infect targets, demonstrating significant effort in social engineering. The fake personas exclusively used phone numbers on WhatsApp with a Hong Kong country code (+852). Links were sent using URL shorteners such as bit.ly to disguise the actual links.

"New York Times" Reporter

In another intrusion attempt, a staff member from the same Tibetan human rights organization was contacted by "Lucy Leung," a persona masquerading as a New York Times reporter seeking an interview (Figure 2) while targeting the individual with an iOS infection attempt. Despite clicking on the link, the target was not infected as they were using an Android device. Perhaps realizing that the target





was using an Android device, the persona sent an Android exploit link, this time disguising it via bit.ly.

Accessing Your Gmail

Besides iOS and Android exploit chains, OAuth is also used in phishing attacks in both targeted operations and generic cyber crime. Recently, we have also seen campaigns using malicious OAuth applications targeting the Tibetan community, potentially in an effort to bypass users who are using two factor authentication on their Google accounts.

On May 31, 2019, a member of the Tibetan Parliament received a WhatsApp message requesting confirmation of a news story. The message included two bit.ly links (Figure 3). The first link sent in the message linked to hxxps://www.energy-mail[.]org/B20V54, which redirected to a Google OAuth application called Energy Mail that requests access to Gmail data. The second link served an Android exploit.

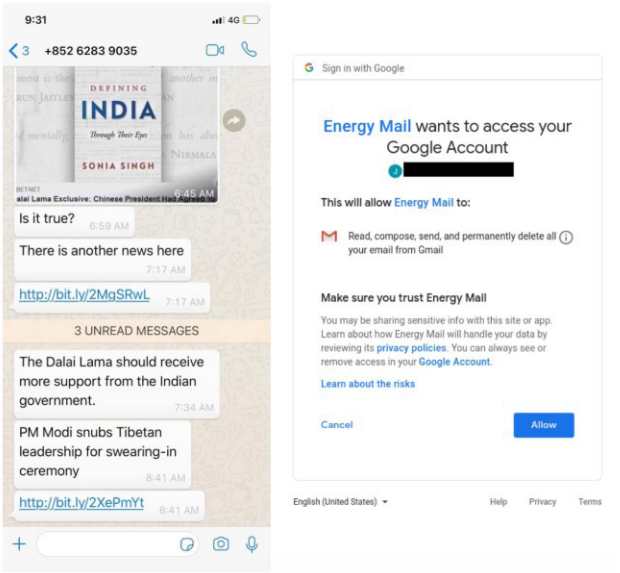


Figure 3: Two bit.ly links were shared where the first one redirected to the Google OAuth application (requesting access to target's Gmail data) while the second link served an Android exploit.

2.2 Solution by TibCERT

Title	Instruction
Don't Wait Update	https://www.youtube.com/watch?v=2PALi87h6yM&t=168s
Think Before You Click	https://www.youtube.com/watch?v=OdJs3zwe4GI

In the past decade, digital security threats towards the Tibetan community have shifted from sending malware as email attachments to phishing and exploit campaigns carried out by POISON CARP. This shows that the operators are changing their tactics in response to the Tibetan community's awareness campaign. It also demonstrates the ongoing digital security challenges Tibetan groups face.

These are some practices highly recommended by TibCERT to avoid becoming a victim of such digital threats.

2.2.1 Don't Wait, Update

We secure our valuables like our wallets, keys, and homes. We know that if left unsecured, they can easily be a target for criminals. So, it makes sense to think the same way about the information stored on all of our devices.

Computers, tablets, phones, and other personal devices hold your emails, as well as important and confidential data. Criminals who get access to this valuable information can steal it, put harmful software on your devices, or both.

What's one easy way to help protect all of this sensitive information? Update your software regularly and as soon as possible when a newer version comes out. What's an even easier way? Set the updates to happen automatically. Don't ignore reminders to

update. Criminals look to exploit vulnerabilities before the software companies can fix it. Delaying updates gives additional time for hackers to access your information.

2.2.2 Think Before You Click

"Did you know this funny video of you is posted online?"

"Click here to read the latest breaking news on the situation inside Tibet"

"An important message from the Dalai Lama"

It is tempting to click on these links, isn't it?

That's because the messages are designed to take advantage of things we care about. Unfortunately, these links are often malicious and will take you to a website where your computer or phone can get infected with a virus.

Don't just open attachments or click on the links you receive in your email, Facebook, WhatsApp, and other communication apps. Unless you were expecting it, there's a strong chance that the attachment or link contains a virus that will dangerously infect your computer or phone as soon as you open it.

As a target community, it is critical that we report these infection attempts immediately to protect and grow our digital security knowledge as a community. Please contact us at info@tibcert.org if you have any questions or notice anything suspicious with your digital devices. Lastly, just as we meditate to clear our minds and help increase our focus, we can do the same for our devices by keeping them updated with the latest security releases, thereby helping keep them free of infections.

3. CHANGES IN TECHNOLOGY FOR TIBET

3.1 Gait Recognition

Watrix, a Chinese surveillance company, developed a new system for gait recognition that can identify people as far as 50 meters away. It even works when a person is not facing the camera or his/her face is covered. In an interview in his Beijing office, CEO Huang of Watrix said, "You don't need people's cooperation for us to be able to recognize their identity. Gait analysis can't be fooled by simply limping, walking with splayed feet or hunching over, because we're analyzing all the features of an entire body."[1]

This gait recognition technology takes a person's silhouette from a video and analyzes the silhoutte's movement to create a model of the way the person walks. However, as of yet, it is not capable of identifying people in real-time. A person has to upload a video into the program. A one-hour long video takes about 10 minutes to analyze. It doesn't necessarily need a specific camera, so footage from any surveillance camera will work.

Beyond surveillance, Huang says gait recognition can also be used to spot people in distress, such as elderly individuals who may have fallen down.

3.2 New "Social Security Card" for Tibetans

According to human rights groups, this year saw Chinese authorities in Tibet expanding the distribution of controversial social security cards across the region, prompting fears that the cards will be used to further tighten control over the Tibetan people.

Recently, Radio Free Asia (RFA) reported on comments from Washington-based International Campaign for Tibet (ICT) that "the cards give access to a wide range of social services including banking, welfare and medical insurance, and will be tied to social-credit system that cuts off benefits to Tibetans deemed disloyal to Beijing's rule." ICT went on to say, "The rollout of the cards reflects the Chinese government's use of personal information as a tool of social control," adding, "In Tibet today, even moderate and mild expressions of Tibetan national identity, religion and culture can be classified as 'splittist' and therefore 'criminal.'" The RFA article also reported that, "Electronic data collected by the cards, which replace a wide range of separate cards already in use, could be used to monitor and 'directly punish individuals with penalties such as loss of employment or pension, torture, imprisonment or

1 https://www.voanews.com/silicon-valley-technology/chinese-gait-recognition-tech-ids-people-how-they-walk

worse,' ICT said."[2]
RFA continued: "Citing Chinese media reports, ICT said that 2.7 million of the new cards have already been distributed across China's Tibet Autonomous Region (TAR), with a total of 3 million set to be issued by the end of the year. 'The new system—which authorities say achieves 'one person, one card,' in TAR—and the rollout of the social credit scheme will strengthen the Chinese government's comprehensive system of 'grid management' (the 'Iron Grid') in the TAR,' ICT said."

3.3 Voice Biometric Collection Threatens Privacy

iFlytek, based in Anhui province, is a major artificial intelligence company focused on speech and speaker recognition. A Chinese company responsible for producing 80 percent of all speech recognition technology in China, they have set up—jointly with the Ministry of Public Security's forensics center—a key ministry laboratory in artificial intelligence voice technology that has "helped solve cases" in Anhui, Gansu, Tibet, and Xinjiang. The company states it can develop artificial intelligence systems that can handle minority languages, including Tibetan and Uyghur.[3]

According to Human Rights Watch, the Chinese government is collecting "voice pattern" samples of individuals to establish a national voice biometric database in collaboration with iFlytek. In fact, in recent years, the Chinese government has stepped up the use of biometric technology in order to bolster its existing mass surveillance and social control efforts. This includes the construction of large-scale biometric databases.[4]

Human Rights Watch goes on to report that, "The collection of voice biometrics is part of the Chinese government's drive to form a "multi-modal" biometric portrait of individuals and to gather ever more data about citizens. This voice biometric data is linked in police databases to the person's identification number, which in turn can then be linked to a person's other biometric and personal information on file, including their ethnicity, home address, and even their hotel records."[5]

4. TECHNOLOGY NEWS ABOUT CHINA

4.1 Huawei Controversy

Huawei is a mainland Chinese technology giant that ranks number one in telecom and number two in global smartphone sales. However, it has recently been more famous as the source of the 2019 US-China trade war. Due to Huawei's close relationship with the Chinese government, their equipment is suspected to have spying tools that are implanted to exploit other countries and companies. Due to this, in 2012, the United States government initially banned US companies from using Huawei networking equipment.[6] In May 2019, President Donald Trump further signed an executive order to cease the use of Huawei products in US communications networks for the security and privacy of the nation. The company was also added to the Bureau of Industry and Security's Entity List in May. The Bureau of Industry and Security is an agency of the United States Department of Commerce that deals with issues involving national security and high technology.

The US trade ban has greatly affected Huawei, as under the terms of the trade ban policy, Google was barred from selling an Android license to them, which meant that Huawei phones could use the base open-source code but would not have access to the all-important Play Store and Google apps. The US offered a temporary reprieve to American companies, allowing them to work with Huawei until August. That reprieve was later extended to November.[7]

For existing Huawei devices, a temporary licence had been issued which allows Google to support and update the Android OS currently running on these devices. As a result, the trade ban has affected

2 https://www.rfa.org/english/news/tibet/controls-08232019152941.html
3 https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy
4 https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy
5 https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy
6 https://www.cnet.com/news/lawmakers-to-u-s-companies-dont-buy-huawei-zte/
7 https://www.cnet.com/news/us-commerce-department-extends-reprieve-allowing-companies-to-sell-to-huawei/

the development of future Huawei products due to the absence of Google tools and support. In order to overcome this issue, Huawei is working on its own operating system HarmonyOS.

In a media interview last month, Richard Yu, the head of Huawei's consumer business, confirmed that Huawei will begin using its HarmonyOS operating system if the situation with the US government does not change . The newly-launched Huawei products (e.g., Huawei Mate 30 and Mate 30 Pro) do not currently have access to Google Play services and support.[8]

4.2 Apple Censorship

Recent activities in mainland China and the protests in Hong Kong have shown that Apple is willing to bow down to the Chinese government's censorship. Apple has censored many apps that raise their voice in support of the pro-democracy movement in Hong Kong and ethinic minorities, including the Uyghur and Tibetan communities.

Earlier this month, Apple removed HKmap.live—an app that pro-democracy protesters and citizens in Hong Kong used to track police activity—from its iOS App Store, after the Chinese Communist Party's flagship newspaper People's Daily published an op-ed criticizing the tool.

Apple also removed Quartz (a news application) from its China App Store after the outlet extensively reported on the protest movement in Hong Kong. Around the same time, Apple began hiding the Taiwan flag[9] emoji from its users in Hong Kong and Macau, since the Chinese Communist Party asserts that Taiwan is formally part of the country under its One-China policy. Previously, the Taiwan flag emoji was only banned in mainland China and not in Hong Kong and Macau. Apple has not given any satisfactory answers on why it has banned these apps from Chinese App Store, just like when they censored 29 Tibetan apps from the Chinese App Store. China's complicated politics present problems not just for Apple and other tech companies, but for any corporation that courts consumers in the country.

4.3 NBA and BlitzChung

On October 4, Daryl Morey, the general manager of the Houston Rockets, shared an image with this slogan: "Fight for Freedom, Stand with Hong Kong."[10] Soon after, he was forced to delete the tweet which stands in support of the Hong Kong protests. Tencent and Chinese state media later halted digital streaming of NBA preseason games, and Morey and the NBA issued an apology. Later, NBA Commissioner Adam Silver revealed he had been asked by Chinese government officials and business partners in China to fire Morey for his tweet.[11]

A few days after the NBA controversy began, the video game company Activision Blizzard suspended BlitzChung. Blitzchung is a professional esports player of the online collectible card game Hearthstone and he hails from Hong Kong. He has played in multiple tournaments and, according to the Hearthstone esports player profile, is ranked seventh in the second season of 2019's Hearthstone Grandmasters for the Asia-Pacific region. On October 6, Blitzchung appeared on the official Taiwan Hearthstone stream after the Grandmasters second season of 2019 ended. During an interview with two streamers, Blitzchung put on a ski mask and gas mask, similar to ones worn by Hong Kong protesters to protect themselves from tear gas, though since banned by the government earlier this month.

The streamers, apparently aware of Blitzchung's motivations, ducked down to hide their faces. For his part, Blitzchung reportedly said in Chinese, "Liberate Hong Kong. Revolution of our age." Blizzard punished Blitzchung by taking away the prize money he won in the Grandmasters second 2019 season and banned him for a year from playing professionally in Hearthstone esports.

4.4 Apple Malware Targeting Minority Group in China

8 https://www.livemint.com/technology/apps/absence-of-google-apps-hurting-huawei-the-most-report-11571638890363.html

9 https://www.wired.com/story/apple-china-censorship-apps-flag/

10 https://www.sportingnews.com/us/nba/news/daryl-morey-tweet-controversy-nba-china-explained/togzszxh37fi1mpw177p9bqwi

11 https://www.si.com/nba/2019/10/17/chinese-government-asked-nba-fire-daryl-morey

In August 2019, Google researchers revealed a series of astonishing iPhone vulnerabilities responsible for compromising a person's phone almost instantly if they visited certain websites. "Simply visiting the hacked site was enough for the exploit server to attack your device, and if it was successful, install a monitoring implant," said Ian Beer, a security researcher at Project Zero.[12] Malicious websites were used to infect victims by tricking them into opening a link that would load one of the websites. According to TechCrunch, "Google said based on their analysis, the vulnerabilities were used to steal a user's photos and messages as well as track their location in near real-time. The 'implant' could also access the user's on-device bank of saved passwords." TechCrunch went on to report that, "The researchers found five distinct exploit chains involving 12 separate security flaws, including seven involving Safari, the in-built web browser on iPhones. The five separate attack chains allowed an attacker to gain "root" access to the device—the highest level of access and privilege on an iPhone. In doing so, an attacker could gain access to the device's full range of features normally off-limits to the user. That means an attacker could quietly install malicious apps to spy on an iPhone owner without their knowledge or consent."[13] The exploit chains affected iOS versions spanning from iOS 10.0.1 released in September 2016 to 12.1.2 issued December 2019. Apple fixed the vulnerabilities in iOS 12.1.4 in February, within a week of Google privately notifying the iPhone maker of the flaws.

According to Google, the websites had thousands of visitors[14] per week for at least two years and the same websites targeting iPhones were also used to target Android and Windows users. This suggests the campaign targeting Uyghurs was far broader in scope than Google initially disclosed. In addition, several news outlets reported that such vulnerabilities had been used to exploit China's ethnic minorities, mainly the Uyghur population, of whom more than a million members have been thrown into concentration camps in the western Xinjiang province. Apple itself confirmed that Uygurs had been targeted through these security flaws. According to Reuters, however, Apple also claimed "the attack 'was narrowly focused' and affected 'fewer than a dozen websites that focus on content related to the Uighur community' rather than the 'en masse' hack of iPhone users described by Google researchers. Apple also said it fixed the issue in February, within 10 days of being notified by Google."[15] Reuters went on to report that Apple said evidence did not support Google's suggestion that the website attacks lasted two years, but rather that they lasted only two months. "Google's post, issued six months after iOS patches were released, creates the false impression of 'mass exploitation' to 'monitor the private activities of entire populations in real time,' stoking fear among all iPhone users that their devices had been compromised," Apple said in a newsroom post. "This was never the case."[16] Throughout their statements, Apple failed to acknowledge the brutal surveillance techniques that Muslim and other religious and ethnic minorities have endured in China for years.

4.5 Facial-Recognition Required to Buy SIM Card

On September 27, 2019, the China's Ministry of Industry and Information Technology (MIIT) announced that telecom carriers must scan the face of anyone applying for mobile and internet service from December onwards. Using facial-recognition technology, the companies will be able to verify that the applicant is indeed the owner of a valid ID. According to Forbes, over the last few years, MIIT has expanded a scheme to link 'real names' to buying and using mobile devices. Registering a SIM card is done with proof of identity, so now all phone activity can be tied to the SIM, resulting in being able to identify the phone user.[17] Forbes went on to report, "From December 1, 2019 onwards, MIIT will mandate 'innovative use of AI' to add technical identity assurance to physical sales channels. Citizens will have their faces checked against enrolled imagery to make sure there's no mischief taking place. The claim is that this will 'safeguard the legitimate rights and interests of citizens' cyberspace.'"[18]

13 https://thenextweb.com/security/2019/09/02/iphone-spyware-campaign-reportedly-targeted-uyghur-muslims-for-2-years/
14 https://techcrunch.com/2019/08/31/china-google-iphone-uyghur/
15 https://www.reuters.com/article/us-apple-cyber-idUSKCN1VR29K
16 https://www.reuters.com/article/us-apple-cyber-idUSKCN1VR29K
17 https://www.forbes.com/sites/zakdoffman/2019/10/12/facial-recognition-will-restrict-mobile-internet-use-for-800m-peoplefrom-december/#4ab03ca27d2a
18 https://www.forbes.com/sites/zakdoffman/2019/10/12/facial-recognition-will-restrict-mobile-internet-use-for-800m-peoplefrom-december/#4ab03ca27d2a