EXTENDED ANALYSIS:

2.3

Civil Society Perspectives and Responses

Over the course of the study we conducted interviews and site visits with nine of the 10 groups participating in our study.[12] The interviews were intended to provide greater context into the perceptions and implications of the attacks documented in this report. The interviews were transcribed and coded to identify emergent themes.[13] This section reflects those themes as section headers, which are as follows:

- Information communication technologies (ICTs) as an enabler and threat to civil society groups
- How our participants perceive digital risks and threats
- The impact of targeted attacks
- Civil society responses to targeted attacks

Each section, in turn, draws on participants' responses, alongside our synthesis, to provide a window into how groups under threat think about and respond to digital threats. In general, we documented groups at different stages of addressing digital security. Some groups had taken on digital security as a core part of their mission before the study began. Others had only begun to notice issues about digital security a few years ago but by the time of interviewing spoke to us about digital threats as a structural problem for their operations. Still, many were in the process of trying to decide on what measures to take, and how to implement them systematically.

ICT: Enabler and Threat to Civil Society Groups

ICTs are central to the activities of the groups, and help them balance an historic asymmetry between them and powerful, well-resourced state interests.

> *[Technology] is the only way you can have any serious impact if you're a size like us and you are trying to go up against the Chinese government which has considerabl[y] more resources than us. So if you want to try to*

12 We were unable to conduct interviews and a site visit with China Group 2.

13 Analysis followed line-by-line open coding methods and grounded theory approaches described in Creswell, J. W. (1998). Qualitative inquiry and research design: Choosing among five traditions. London, UK: Sage.

have an impact, technology is the leverage.[14]

The two large human rights organizations in our study both operate distributed programming across multiple countries with hundreds of staff and partner organizations. The size and complexity of these operations makes these groups highly reliant on technology.

> *Now we do work in more than 80 countries at any given time, and we have staff based in many cities across the world.*[15]

The theme of diaspora communications was central to groups related to Tibet and China. The Tibet Groups, for example, find that technology enables them to reach into restricted environments from "safe" areas overseas.

> *In comparison to other communities, there is almost nowhere that is so physically separated because of the restraints imposed by China….Even in Pyongyang, you got foreign journalists...Tibet is just closed off….Technology is the only way that that can be bridged.*[16]

ICTs are also the primary tool that organizations used to connect with the highly distributed and fractured community in the Tibetan diaspora and in Tibet.

> *Those of us born and raised in exile, and certainly our parents and other generations, crave to go home to this land they are so attached to. Then technology comes along and it's like BOOM! You can have it all…on some level even though the Chinese are still there and physically we can't do it, but in this other space we can.*[17]

14 China Group 1, Director, 2010

15 Rights Group 2, Technical Officer, 2011

16 Tibet Group 1, Program Officer, 2011

17 Tibet Group 1, Director, 2011

WECHAT: CONNECTIVITY AND RISKS

WeChat is a mobile chat application developed by Chinese company Tencent, which has gained huge user numbers around the world with a high concentration in China. Tibet Groups cited WeChat, which is highly popular in their community, as an example of the tension between connectivity and security. This connectivity was seen as beneficial, but not without risks.

"New ground shows up like WeChat...and it threatens to both undermine [our efforts] and offers us some ideas for what it is people want and [what they're] willing to compromise for the sake of connection."—Director, Tibet Group 1

"Tibetans in India and Nepal, Tibetans in the West are all being connected by using the same app...and forging these new connections...in some ways, we're seeing really good things come out of it in terms of all the news we're getting from Tibet and seeing all the footage from the self-immolations and protests coming from WeChat and in that sense it's becoming important, but people are not so attuned to the risks."—Program Officer, Tibet Group 1

Tibet Groups voiced concerns over the increasing popularity of WeChat due to censorship and surveillance requirements on companies operating in China, and the close relationship between Tencent and the Communist Party of China. Adding to these concerns are a series of documented incidents of Tibetans in Tibet being arrested for content they shared on WeChat, like images of HHDL.

Civil society and its champions are not the only groups who felt that technology could enable movements to push back against the status quo. A Tibetan group noted that they thought the Chinese government, was also very concerned about its potential.

> *...self immolations and protests...the Tibetan cultural pride, the songs...this is the reason the Chinese are cracking down so hard and going after everyone ..... the censorship and the surveillance is...[happening] because the technology has showed them what's possible. There is a movement now where there wasn't one or where it had almost disappeared before... the technology has enabled that.*[18]

Yet the ability to connect is constantly eroded by efforts to monitor and interfere with groups' activities. Participants also recognized that their reliance on technology intro-

18 Tibet Group 1 Director, 2011

duced new risks of monitoring, coercion, and electronic attack.

> *[Technology is] this funny thing where it's a life line, and then it's...maybe your ticket to jail.*[19]

Groups need members of their communities to maximize the use of ICTs but also to do so securely.

> *We...need this technology, but we need everybody to know how to use it and be able to be secure and be safe.*[20]

Targeted digital threats are also changing how some CSOs see the promise of technology.

> *I think that civil society is feeling the heat around targeted attacks and surveillance and I think it's affecting the public sphere and our ability to feel comfortable communicating in what used to be understood as a free and open medium.*[21]

In practice, CSOs are in a constant process of navigating through new communication environments, and tradeoffs between connectivity and security. Contrasting theories have popularly characterized ICTs either as "liberation technologies" that can empower political movements, or as levers of control for governments to suppress these very same movements.[22] Our participants suggest that the reality is somewhere in between.

How Civil Society Groups Perceive Risk and Threats

We tried to elicit participants' informal "threat models" as a precursor to understanding how these models shaped their response to digital risks.[23] All of the groups in our study work on political issues that can potentially be seen as threatening to specific authorities. The context of this work makes many groups perceive the attacks against them as politically motivated.

19 Tibet Group 1, Director, 2011

20 Tibet Group 1, Program Officer, 2011

21 Rights Group 2, Technical Officer, 2014

22 See, e.g., Diamond, L. "Liberation Technology," *Journal of Democracy* 21, no. 3 (2010): 69–82; Morozov, E. *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

23 A threat model assesses the risk and relative impact of threats against an entity that are specific to the context in which it is situated.

Although political concerns were a backdrop to the attacks, groups tended to focus on the tactical goals of the attackers rather than the greater political objectives. Groups described the probable goals of attacks as efforts to "hinder our operations," "keep an eye on things," or cause as much "inconvenience and chaos as possible [to] somehow affect our ability to do what we do."[24]

While groups shared similar views on the operational objectives of attackers, their sense of risk stemming from attacks depended on the physical proximity of their adversary. A program manager with extensive field experience working with CSOs in multiple countries explained that groups operating within the jurisdiction of an adversary have greater concerns over physical security and other direct interference from authorities.

> *...in many places it's a very physical sort of thing. Our biggest challenge...[was when]...local authorities wandered in and took computers. So it's not like we expect the attacks to be all coming in over the wire. In most places where we operate it's probably not even the easiest place for them to get at although it is certainly a lot more subtle.*[25]

If a group is situated outside of a physical jurisdiction controlled by an adversary then targeted digital threats may be a higher priority concern than physical threats.

> *Take for example Ukraine where they aren't necessarily expecting a lot of challenges with their local government, but they might be a target for cross border action, that is one of the places where the digital threats become a particular vector or focus rather than just one of the many things that they are thinking about.*[26]

DIASPORA AND EXILE COMMUNITY THREAT MODELS

Many of the participants in our study working on China and Tibet issues are embedded within geographically distributed diaspora networks. Their missions often include collecting information from closed areas "inside," while transmitting other information back in. As the director of an organization working on China explained:

24 Rights Group 1, Chief Technical Officer, 2011; Tibet Group 2, Executive Director, 2014

25 Rights Group 1, Program Manager, 2014

26 Rights Group 1, Program Manager, 2014

> *Our main target and focus is on the mainland. And so the people who [we] are trying to promote, the people who we are trying to give platforms for their issues and their problems and their voices are inside.*[27]

A central concern of these groups was the security of the bidirectional flow of information to and from at-risk persons in China and Tibet. A group working on China perceived its adversary as primarily interested in this information exchange.

> *Anyone who doesn't want [our organization] to be able to safely and securely get information from inside...and send it back in. What kind of information? Individual case information, human rights information... Anyone who has an incentive not to have people know about it would have the incentive to compromise our operations and make it hard for us -- and that's a lot of people.*[28]

Due to the antagonistic response these activities elicit from the Chinese government, the Tibet and China Groups generally perceived the actors behind targeted digital attacks on their community to be directed by or related to agents of the PRC.

> *I think in most cases, [the staff] believe it's coming from China.*[29]

Tibetan groups in exile perceived Tibetans living "inside" as having the highest likelihood and impact of harm from digital attack. To demonstrate the potential consequences of targeted digital threats, a Tibetan security trainer explained how he presents the connection between actions outside affecting at-risk groups inside Tibet.

> *I kind of force them into thinking about like the risk associated with Tibetans inside Tibet, and also kind of like stress the fact 'We are in a free country, we don't have to worry about ourselves...What can the Chinese government do to me? Nothing. But what happens when you have done something that's harming somebody else inside Tibet?' ...that's when a lot of people think about it a little more.*[30]

The threat models of groups working on China and Tibet show a priority given to digital threats due to the proximity of these groups to their perceived adversary and the years of persistent attacks they have experienced.

---

27 China Group 1, Director, 2010

28 China Group 1, Director, 2010

29 China Group 1, Technical Project Manager, 2014

30 Tibet Group 1, Digital security trainer, 2013

> *...most communities just aren't...under as persistent, sophisticated and threatening attacks, so they just have not gotten to the same place in prioritizing digital security.*[31]

Our study exclusively addresses digital threats and does not cover all potential threats a group may face. While digital threats are a primary security concern for the majority of groups in our study, they are just one piece of a holistic risk environment for CSOs.

Impact of Targeted Threats on Civil Society Groups

Most participants were clear that they saw potentially severe consequences from targeted digital attacks, with the greatest danger being to communications with those "inside," and hence vulnerable to arrest or harassment. Nevertheless, a few participants surprised us by noting that their organization downplayed the possibility of negative consequences from attacks (or had done so in the past). Often this reaction took the form of citing the 'openness' of their organization's work, and suggesting that there was 'nothing sensitive' in their exposed data.

> *This is an organization predicated on virtues of transparency...when I first came here there were a lot of conversations like, 'Why should we encrypt our email, we are not hiding anything.'*[32]

As evidence of attacks against that human rights organization piled up, however, perceptions began to change.

> *...there has been a sea change in the four years since I have been here...they recognize a riskier threat environment and how it is dealt with.*[33]

Awareness of risks was, however, still a work in progress.

> *...in the last year or two any organization that I have been working with in a closed society or dealing with sensitive topics at least has some sort of hazy consideration that this stuff should be a concern and that's maybe a change from*

31 Tibet Group 1, Director, 2011

32 Rights Group 1, Program Manager, 2014

33 Rights Group 1, Program Manager, 2014

when I first started. But...it's very piecemeal.[34]

These responses raise an important issue: the relationship between digital compromises and the use of the compromised information by adversaries is indirect. Unlike the consequences of physical threats, which are often directly observable to a non-expert, the most serious impacts of digital threats are typically at least one step removed from the technology that has been exploited. Making the link between technological threats and "real-world" harm can be challenging, in part due to limited evidence.

> *... [there has] been little evidence of the direct impact on people's safety as a result of some of these threats.... [but] our understanding of how surveillance and repressive practices have operated even in pre-digital times provides us with sufficient evidence to understand that there may be a connection. I believe that there has been an increase on the reach of this harm by specialist state actors...*[35]

CONNECTING SURVEILLANCE AND HARM

We often heard stories of arrest and detention from groups in the study (and through other Citizen Lab projects) that appeared to be linked to electronic surveillance.

Members of the Tibetan community shared with us accounts of Chinese authorities confronting Tibetans with call records and chat transcripts during interrogations. Meanwhile, research on Ethiopia has revealed that detainees have been presented with similar evidence during interrogations.

In Syria there are also reports of interrogators presenting detainees with records of communications, and cases where accounts of detainees are used to seed malware to contact lists.

In Bahrain, meanwhile, activists were arrested after posting pseudonymous tweets critical of the government. The real identities of these persons may have been discovered by authorities through a technique in which an attacker sends the pseudonymous Twitter account a link to a webpage containing an embedded remote image. When the victim clicks on the link or opens the email, their IP address is revealed to the attacker. Authorities can then link the IP to the target's true identity through their ISP.

We strongly suspect that these cases are only the tip of the iceberg, and that the digital element in many cases of harm goes unrecognized due to lack of investigation, not lack of incidents.

34 Rights Group 1, Program Manager, 2014

35 Rights Group 2, Technical Officer, 2014

We also think, however, that by downplaying the consequences of targeted digital threats, some participants were showing us something interesting about the resilience and adaptability of their communication styles, which have co-existed with an adversary that has used extensive monitoring for many years.

> *...it can be a nuisance, it can be a distraction, it can waste time, but...in the grand scheme of things, it's not as though the movement on a whole operates in a way that is dependent upon secure conversations.*[36]

Nevertheless, the same participant was very clear that serious (even physical) harm could come to individuals and groups "inside" through targeted attacks against them or their contacts.

PSYCHOLOGICAL IMPACTS AND COPING STRATEGIES

While tracking the consequences of a targeted attack for networks of trust and reputation can be challenging and require investigation, some participants spoke in detail about the psychological impact of compromise.

> *It was quite upsetting. I think it sort of paralyzed us emotionally—the two of us that were affected—for a few days.*[37]

In this incident, the emotional harm was perceived as more impairing, and less easily mitigated, than the breach to the computer system.

> *...the act of cleaning our computers was something that was relatively straightforward...but it was the emotional impact that sort of threw us.*[38]

Further work is needed to document the connection between targeted digital threats and psychosocial strain to move towards a more complete understanding of how targeted individuals and organizations evolve and adapt their coping strategies. One interesting coping strategy prevalent among Tibet Groups was to explain attention from adversaries as a signal that their work was important, and was having an impact.

> *The reason you are a target is because you are doing something that is bothering somebody and to be proud actually of the work that you do that has drawn the attention of these people who clearly want to mess us up somehow.*[39]

36 Tibet Group 2, Director, 2014

37 Tibet Group 2, Director, 2014

38 Tibet Group 2, Director, 2014

39 Tibet Group 2, Director, 2014

As one participant put it, the challenge was to balance the frustration of being compromised with feelings of encouragement:

> *…we work so hard the entire day and then at the end of the day when you find out that your website has been attacked and people can't get access to it, you get frustrated, but at the same time you also get more encouraged to know that… feeling that your work is making an impact and the Chinese government has to go to the extent of spending time following us and attacking us and spending large amounts of money just for that.*[40]

BEING TARGETED: A TEACHABLE MOMENT

Beyond trainings and awareness campaigns, what brought threats home, unsurprisingly, was being targeted or compromised. Being attacked personalized the problem, and turned warnings into tangible concerns.

> *[It] is visible for users in places that they understand—your email, your Twitter account—even if they don't understand the implications, the connections...they now see it as something real and personal.*[41]

Tibet Groups felt that the persistent targeting of their community has helped them raise awareness of digital security and highlight the need for vigilance.

> *It has made Tibetans more aware of the potential of the Chinese government. We always think about the Chinese government creating problems for us diplomatically, we don't think of the cyber world...and how they can maneuver their way into it.*[42]

> *[The attacks]... give us as a reminder to be more careful.*[43]

Groups made it clear that greater awareness is a work in progress, and that documenting the connection between attacks and specific harms to individuals and groups is a promising way forward.

> *The basic goals should be to get people to realize that these threats are real... the*

40 Tibet Group 3, Editor-in-Chief, 2014

41 Rights Group 2, Technical Officer, 2014

42 Tibet Group 3, Editor in Chief, 2014

43 Tibet Group 5, Program Officer, 2014

chain of events from clicking on something, to some person being in peril. [44]

Civil Society Responses to Targeted Digital Threats

As groups struggled with targeted threats, many placed an emphasis on awareness raising and user education as a primary method of responding. These kinds of strategies are important for civil society and applicable to a variety of problems. The fact that many of the digital threats they experience rely on social engineering makes this a promising direction. However, responses from the groups also suggest that resource constraints, and limits on available technical expertise, may have constrained other avenues of response.

RESOURCE AND CAPACITY CONSTRAINTS

The most commonly mentioned challenge to addressing digital threats was, unsurprisingly, resource issues in general, and technical resources and skills in particular:

> *Every community with a struggle is under-resourced, and if this hasn't moved up the priority list, they don't have the capacity to do this type of stuff or implement it or there's not even enough awareness that is needed for them to be able to [get] people to pay attention.*[45]

Organizations in the Global South

These challenges are especially acute for groups in the global South. All Tibet Groups in our study had their operations or a portion of their operations based in Dharamsala, India. In this context, the groups are operating within a refugee community grappling with persistent targeted attacks and conventional development challenges. Resources are sparse. These groups cannot afford enterprise computing infrastructures, or the expensive security solutions adopted by larger, well-resourced counterparts.

Complicating these challenges is the problem of "brain drain" of technically skilled people in the community. Participants told us many Tibetans with specialized technical training

44 Tibet Group 1, Program Director, 2011

45 Tibet Group 1, Director, 2011

leave Dharamsala in search of better job prospects elsewhere. Tibet Groups saw the need to create opportunities for Tibetans with technical skills to work in the community:

> *[Tibetans living in exile in India] are essentially a refugee population and all these folks want to get jobs. So, if we can actually bring them in and give them jobs in supporting their own community, that's kind of a goal.*[46]

Others, on the same topic, suggested that the problem was improving, slowly:

> *I think now it's coming up slowly and slowly, but there was a time in the Tibetan community where we really lacked webmasters, where we really lacked people who are well equipped and who have good knowledge in terms of Internet security.* [47]

These challenges are not unique to the Tibet Groups. Rights Group 1 explained that local partners supported by the group faced similar technical capacity difficulties:

> *Security is hard and it's much harder than it needs to be….the challenge of trying to keep your stuff in some kind of secure state as is currently defined is just well beyond what any typical partner organization is able to deal with…For most of our partners they are lucky if they have a young guy who understands a bit about computers.*[48]

A particularly common problem for groups in the global South is the use of pirated software (unpatched or pre-backdoored software is often a source of insecurity). The use of pirated software is widespread in the Tibetan community due to prohibitive licensing costs. Similarly a program officer in a large rights group explained it is difficult to convince a local partner to purchase a software license "when you can jump out to the local market, [and] for a dollar buy a disk."[49]

Larger Organizations

Two of our participating organizations, Rights Groups 1 and 2, had significantly higher technical capacities and financial resources, and they approached information security in a manner similar in some ways to a large company. For example, the groups have senior management in charge of security and technology, IT support teams / help desks, and occasionally hire companies to provide security consultations

46 Tibet Group 1, Program Director, 2011

47 Tibet Group 5, Program Officer, 2014

48 Rights Group 1, Program Manager, 2014

49 Rights Group 1, Program Manager, 2014

and incident response services. However, although the size and resources of these groups afford them certain advantages over smaller groups, they experience equally vexing security challenges.

The complexity of global operations and distributed staff and partners creates problems for introducing and sustaining security awareness, even as attacks seem to increase:

> *We have seen a colossal uptake on attacks on the home office or we are just much more aware of them than we used to be. We anticipate that such things are also happening at the field office level and to our partners, but we have much less visibility into that.*[50]

The lack of network visibility among in-country offices was cited as a particular challenge:

> *We don't have a unified network with all our field offices… so we don't have the same enterprise level of security and capacity there…[the field offices and NGO partners] have to face a range of threats that are from the physical world as well.*[51]

Both groups face challenges adapting technology policies for regional offices and partner organizations. Rights Group 2, for example, contended with securing its head office and maintaining awareness of threats faced by field offices:

> *There's not a lot of security awareness in the organization. There's ... small pockets of knowledge, but the rest of the organization will prove to be the weakest link….people don't understand, especially people that work in the field don't understand the sensitivity of the work the organization does, so they tend to be a bit more lax about... certain things.*[52]

Bureaucratic processes were seen as hindering the adoption of new security policies, given the challenge of informing decision makers about emerging security issues:

> *I think it has been very top-down, you know some [policy] comes from the top, they go to the bottom and there is no way to inform what's going on in the decision process.*[53]

50 Rights Group 1, Program Manager, 2014

51 Rights Group 1, Program Manager, 2014

52 Rights Group 2, Technical Officer, 2014

53 Rights Group 2, Technical Officer, 2011

TRAINING AND USER EDUCATION

While the two large groups were able to invest in security appliances and dedicated technology support, the other groups in our study focused on user education and awareness as the primary security strategy.

The majority of groups focused on internal training programs and training with partner groups. Five were able to conduct these trainings themselves,[54] while four others[55] drew on third-party support. These trainings varied widely, ranging from short explanations of security policies to sustained user education programs.

Several key themes emerged from our interviews about digital security trainings: the value of understanding the local context, the need for training based on organization-specific threat models, and the value of focusing on behavior rather than simply teaching a wide range of tools.

Training informed by local context and threat models

While user education and training were a major part of groups' strategies, most highlighted the importance of situating trainings in local context and using accessible language and concepts.

> *If we could break it down for people in a way that they understand, if we could give them metaphors and other ways to understand what exactly this means for us, and paint the bigger picture, it has an impact.*[56]

Rights Group 1 explained that conducting formal risk assessments of its partner organizations was key in developing appropriate educational strategies.

Other groups engaged in training shared similar comments and noted the importance of ensuring trainings are in line with both technical and contextual realities. Several interviewees pointed out that keeping abreast of new technical developments and context-specific risks was challenging and time-consuming, highlighting the value of intermediary organizations that perform this role within a particular targeted civil society context. Indeed, Tibet Group 1 went so far as to structure its mission to focus on digital security awareness and education programs for the Tibetan community. The

54 Rights Groups 1, 2; China Groups 1, 3; Tibet Group 1

55 Tibet Groups 2, 3, 4, 5

56 Tibet Group 1, Director, 2011

group provided training support to all the other Tibetan organizations who participated in the study.

Moving Beyond Tools

All of the groups identified a common set of user practices for preventing infection of malware: not opening unsolicited attachments, being careful with web links, keeping systems up-to-date, and generally remaining vigilant online. Explaining the safe and secure use of tools was an aspect of training, but many groups focused more on how to change behaviour and develop a security mindset rather than train specific tools.

> *[We are] trying to equip people with a different mindset, so that they are changing their behaviors...so they...run through a mental filter before doing something.* [57]

Tibet Group 1, which regularly provided trainings to its peers, was particularly adamant about the need to focus on user behaviour over specific tools:

> *We would really like to see resources shift from trying to mitigate problems through tools, to mitigating problems through education and educating people about their practices.* [58]

The Tibet Groups felt that user education had to be a community-wide effort and not something isolated to particular organizations or individuals. For example, some Tibetan groups have been promoting a "Detach from Attachments" campaign that encourages users to move away from sharing documents through email attachments and shift to alternative cloud-based platforms like Google Drive. The campaign uses a mix of humor and references to Tibetan culture and is a good example of user education that is connected to a specific threat model and local context.

Encouraging behavioural change and implementing new organizational policies can be challenging. Tibet Group 5 explained that while malicious attachments were a priority threat for the group, moving to alternative document platforms was difficult due in part to generational gaps in the group's membership. Users from older generations, they explained, were resistant to changing familiar practices, like the use of attachments.

Understanding these organizational challenges and breaking down trainings into simple incremental steps that can be adapted to specific environments were identified as keys

57 Tibet Group 1, Director, 2011

58 Tibet Group 1, Program Director, 2011

to success. A Tibetan security trainer described the importance of showing people small victories from their point of view and demonstrating how they can learn to achieve ICT objectives in ways that are safe and secure, but also do not appear too difficult for them to use in their daily workflows.[59] Others agreed, saying that their goal was to find techniques that made it "as simple as [possible] to do the right thing..."[60]

Indeed, there were some cases where, if implemented effectively, modest behavior modifications could have a considerable impact. While we observed organizational challenges in implementing practices like "Detach from Attachments," based on what we have seen, the campaign could be effective against some of the current threats against the Tibetan community. More than 80% of malware submitted to us by Tibet Groups used a malicious email attachment. Furthermore, for two of the Tibet Groups in our study, simply not opening attachments would mitigate more than 95% of targeted malware threats that use email as a vector.[61]

However, this is just one mitigation strategy focused on a single vector of attack. Threat actors are highly motivated and will likely adapt their tactics as users change their behaviors. For example, it is possible that if every user in a particular community began to avoid opening attachments, attackers would move on to vectors such as watering hole attacks or attacks on cloud-based document platforms.

As the groups themselves noted, user education and awareness-raising activities need to be ongoing, and must be informed by local context, threat models, and the latest technical information.

59 Tibet Group 1, Security Trainer, 2013

60 Rights Group 1, Program Manager, 2014

61 This determination is based on two groups that had submitted at least 40 emails.