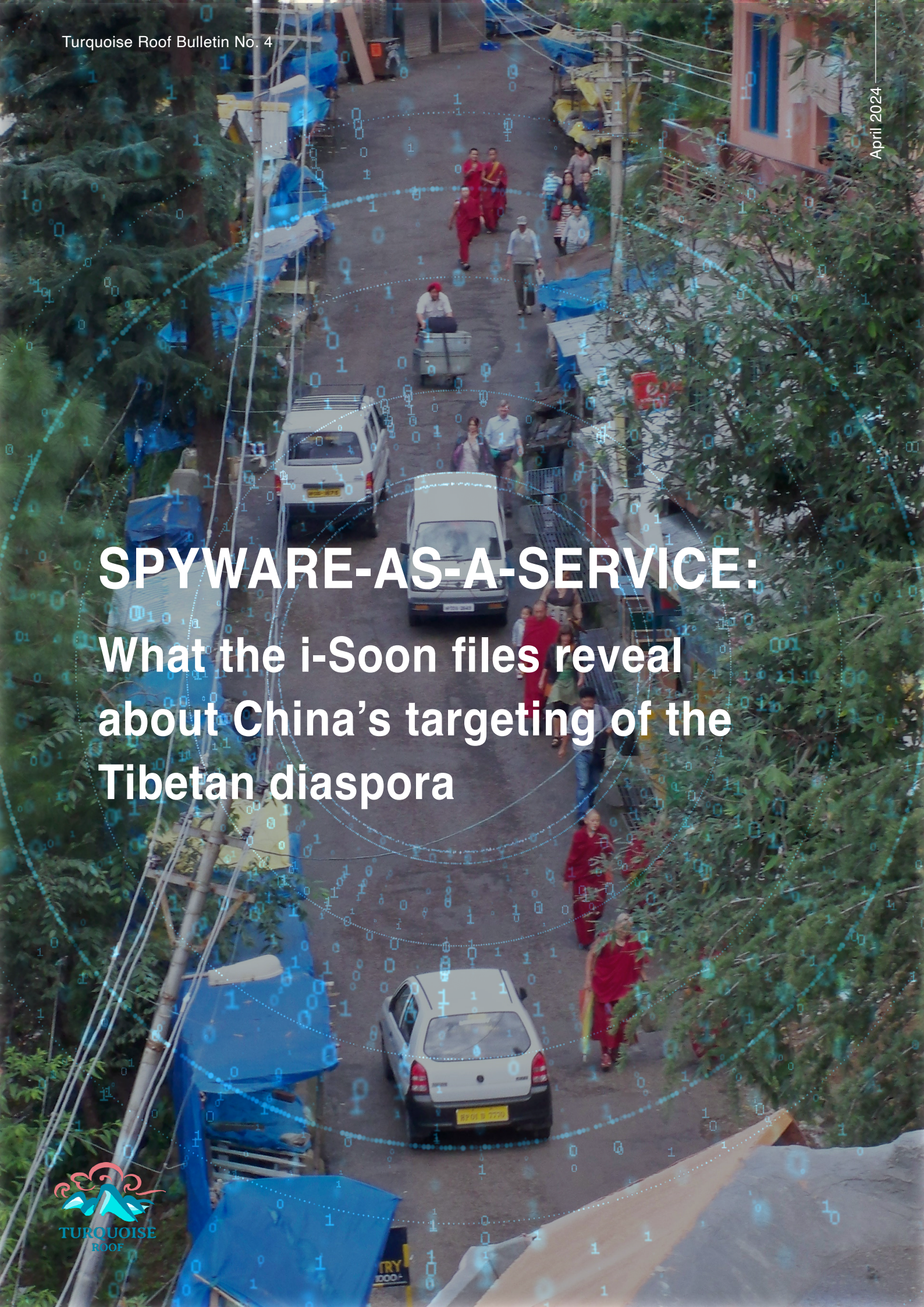
April 2024



SPYWARE-AS-A-SERVICE:

What the i-Soon files reveal about China's targeting of the Tibetan diaspora

TURQUOISE ROOF

Preface

The pervasive spread of digital surveillance technologies and their deployment against vulnerable communities has garnered high-level attention from prominent Western governments, including those of the United States, the United Kingdom, France, and Canada. Incidents involving targeted surveillance executed by entities like Israel's NSO Group through Pegasus malware have ignited widespread concern. These cases have spotlighted the potential of such technologies to undermine human rights and to erode the democratic fabric of societies.

Governments are increasingly incorporating cyber operations into the arsenal of statecraft. This sophisticated integration combines open-source intelligence, geospatial intelligence, human intelligence, and cyber espionage with artificial intelligence, allowing for the gathering and analysis of ever-expanding data sets. Increasingly, such operations are being outsourced. This report scrutinises one instance of outsourced cyber intelligence capabilities, brought to light by the leak of internal documents from a Chinese cybersecurity firm.

Executive Summary

In February 2024 a leak of documents from i-Soon, a Chinese cybersecurity firm tied to the nation's security apparatus, gave new evidence of People's Republic of China's (China or PRC) large-scale and shadowy cyber espionage activities. The data dump provides valuable insight into the priorities of the Party state in hiring hackers to target peripheral communities, including the Tibetan exile administration in Dharamsala, Uyghurs in the diaspora, pro-democracy advocates in Hong Kong, as well as official entities in neighbouring countries such as the Mongolian police, and India's customs agency.

The leak demonstrates both operational continuity and a steady evolution in China's strategic deployment of targeted surveillance technology. For long-time observers, the leak provides significant evidence confirming that China's targeting of vulnerable individuals and groups through commercial Chinese cybersecurity companies extends well beyond PRC borders, infiltrating hundreds of official and individual systems.

Examination of the i-Soon files reveals that the Tibetan administration in exile and the Dalai Lama's Private Office in India were among the targets of sophisticated cyber espionage. i-Soon, whose biggest clients included the Chinese police, the People's Liberation Army, the Ministry of State Security and the Tibetan regional authorities based in Lhasa, harnessed advanced technological capabilities for data mining and communication pattern analysis.

Data from the i-Soon leak has been linked to previous Advanced Persistent Threats (APT) campaigns targeting the Central Tibetan Administration (CTA), the Private Office of the Dalai Lama, and Tibetan and Uyghur civil society networks. Palo Alto's Unit 42 were the first to report, with a high degree of confidence, that i-Soon is connected to an APT group known as Poison Carp.[1] This attribution is based on forensic evidence surfaced in the i-Soon dump linking the company to targeting infrastructure attributed by Citizen Lab to Poison Carp[2], a Chinese threat group hitherto principally known for targeting the mobile phones of Tibetan[3] and Uyghur[4] social movement networks.

The targeting of the mobile phones of CTA officials from 2018 onwards represents a significant shift in the tactics used by threat actors, signalling an adaptation to modern communication methods and an understanding of the increasing reliance on mobile devices for both personal and professional activities. i-Soon's compromise of mobile devices would facilitate the collection of large amounts of highly sensitive information about civil servants, which would put them, and those in their social network, at significant risk.

A key white paper found in the i-Soon data delineating its product's capabilities utilises the compromised email inboxes of exiled Tibetan individuals as a case study, demonstrating the product's ability to manage and analyse "massive" data collections on a "terabyte-scale." This capability is tailored to satisfy the extensive demand of China's intelligence agencies, domestic- and foreign-facing (i-Soon's clients) to mine through substantial volumes of intercepted email data and to intricately map the social networks of targeted individuals.

The use of novel intelligence tactics against diaspora populations before global deployment also suggests an approach to cyber operations in which vulnerable populations serve almost as laboratories for China to refine its espionage capabilities. When applied to operations directed at Dharamsala, such testing could not only yield intelligence about Tibetan exiles, but also enhance the sophistication of China's cyber arsenal, reducing the risk of detection and attribution in global operations against better resourced defences.

The analysis of the interpersonal relationships of target networks of Tibetans in exile deployed by i-Soon mirrors the oppressive securitisation methods used in Tibet. As i-Soon's customers include the Public Security Bureau of the Tibet Autonomous Region, it is feasible that the web of personal and professional connections surfaced from compromised inboxes of senior Tibetan civil servants in India could have been later ingested into a known big data policing platform. This platform is instrumental in a campaign that criminalises even moderate cultural, religious expressions, language rights advocacy, and crucially, surfaces links to exile Tibetan networks.

The Central Tibetan Administration and the Dalai Lama's personal office have been under digital threat for twenty five years, with the GhostNet operation that infected computers in the Dalai Lama's office making global headlines in 2009. The first public recognition of these security challenges in the early 2000s pre-dated warnings from Western intelligence services about such intrusions. Today's threats, however, are defined by their complexity and stealth, exploiting both known and unknown vulnerabilities in networked systems.

i-Soon data files offer a glimpse, perhaps for the first time in the public domain, of the upstream APT analytics capabilities of the Party state, offering a new understanding of the processing and utilisation of data exfiltrated by APT groups for i-Soon's Chinese intelligence and military customers. This also highlights the involvement of commercial enterprises in cyber espionage activities including significant insight into Beijing's use of complex AI-driven surveillance systems[5] to enforce political controls over PRC ethnic minority populations, not just within its own borders, but also internationally, in the diaspora(s). Demonstrating sophisticated technologies on vulnerable peripheral communities like Tibetans and Uyghurs appears to be a strategic move for corporate entities like i-Soon to advance their corporate interests.

The i-Soon leak highlights the cybersecurity threats faced by the Tibetan administration in exile, which not only emphasise the imperative for cybersecurity but also the profound consequences of cyber espionage on vulnerable populations. They accentuate the need for heightened vigilance and international cooperation to fortify the digital defences of those at risk.

Digital transnational repression targeting the Tibetan and Uyghur diaspora serves as a "canary in the digital coalmine" for democracies. Early warning capacity built into these digital diasporas could have surfaced these threats and led to a coordinated response in the West much sooner. Reports by Tibetan and Uyghur sources detailing digital threats from Beijing predated by several years Western intelligence's public warnings of China's cyber espionage targeting the corporate sector.

This report is structured in three parts:

- Part One outlines the historical context of Chinese intelligence agencies targeting Tibetans and the CTA, providing insight into the background of these cybersecurity threats.

- Part Two evaluates the capabilities of a key analytical tool used by i-Soon for email analysis in decision-making processes. This section explores how the tool operates, illustrating its use in targeting specific Tibetan institutions and individuals. It also examines how the tool's methods align with the tactics traditionally used by the Chinese intelligence services. Additionally, this part contextualises the deployment of such tools against minorities, including Tibetans and Uyghurs, within the broader strategy of China's transnational repression.

- Part Three offers final thoughts, reflecting on the broader implications of the i-Soon case study. It discusses the growing danger that arises from the spread of commercially developed, state-backed digital surveillance technologies.

Contents

Part 1: Targeting Tibetans: Background and Context

On 16 February 2024, a significant breach of the People's Republic of China's (PRC or China) cyber espionage capabilities was identified when a substantial volume of sensitive documents seemingly connected to a cybersecurity firm affiliated with Chinese intelligence agencies surfaced on GitHub.[6] The disclosure comprised materials reportedly emanating from i-Soon, also known as Shanghai Auxun (上海安洵), a Shanghai-based commercial entity deeply enmeshed in the intricate and largely non-transparent commercial sector of cyberspace espionage within China.

This release presents a window into the covert realm of Chinese commercial cyber espionage, revealing the intricate and comprehensive intelligence operations, tactics, and likely targets of Chinese overseas intelligence activities. The exposed documents provide an inventory of digital surveillance tools and technological apparatus, drawing parallels with the historic revelations by Edward Snowden concerning the National Security Agency's cyber capabilities.

The breadth of the leak, entailing more than 570 files, offers unprecedented transparency into the modus operandi of the commercial ecosystem that buttresses Chinese state-sponsored cyber espionage initiatives. Included are internal communications, corporate records, and various artefacts that illuminate the enterprise's role in creating bespoke cyber espionage instruments.

The leaked archive outlines how enterprises such as i-Soon develop unique surveillance technologies and infiltrate systems, serving the Chinese government's surveillance and espionage objectives. The documents provide insights on how i-Soon markets its claimed technical abilities against key figures and groups such as the Tibetan diaspora, the Uighur community in exile, and pro-democracy advocates from Hong Kong — all targets of transnational digital repression by the Chinese state.

A key whitepaper delineating i-Soon's product capabilities uses the compromised email inboxes of exiled Tibetan individuals as a case study, demonstrating the product's capabilities and tailored to satisfy the extensive demand of China's intelligence agencies (i-Soon's clients) to mine through substantial volumes of intercepted email data. The platform is engineered to facilitate investigations into an individual's "interpersonal network" and supports "semantic analysis" of communicative patterns to deduce additional intelligence.

The documents and conversations in the i-Soon archive also suggest that the cyber operations advanced by suppliers like i-Soon are attaining a heightened level of sophistication and stealth. Their arsenal encompasses an assortment of tactics, including the deployment of zero-day exploits (a vulnerability or security hole in a computer system unknown to its owners, developers or anyone capable of mitigating it) and specialised hardware designed for the remote compromise of computers and communication networks. It underlines the pivotal role of an approach known as meta-synthetic engineering, outlined in this report, which integrates diverse streams of intelligence – ranging from quantitative data like signals intelligence to qualitative inputs such as human intelligence – into a unified analytical construct ("comprehensive" or integrated analysis).

Tibetan groups operating in exile have faced cyber espionage by the PRC military intelligence for nearly a quarter-century. These cyber intelligence operations were previously highlighted in the 2009 GhostNet report[7] by Citizen Lab and the SecDev Group, which unveiled the extent of China's capabilities and targets spanning South Asia and beyond.

The i-Soon dossier grants journalists and researchers across the globe another rare and crucial perspective on the evolution and proliferation of the commercial cyber espionage landscape in China. The trove of documents underscores the intricate challenges faced in protecting online freedom and security against an ever-expanding arsenal of state-sponsored cyber espionage tools.

I. The Central Tibetan Administration and digital transformation

The Central Tibetan Administration (CTA) serves as the representative body for Tibetans living in exile, with a pivotal role in global advocacy for Tibetan rights and issues. Dedicated to the preservation and promotion of Tibet's cultural and religious heritage, the CTA disseminates information to raise awareness and generate international support for Tibet.. Because of this mission, the CTA is subjected to a plethora of challenges, including surveillance and cyberattacks from the People's Liberation Army and various Chinese intelligence bureaus.

The CTA garners significant attention from the PRC as it is perceived as a threat to Chinese strategies and interests in Tibet. Operating as a government in exile, the CTA actively practises statecraft[8]— an action viewed as undermining the PRC's claim over Tibet and exacerbating concerns over its control of the globally scattered Tibetan diaspora.

The escalation of cyber operations against the CTA by China's military and intelligence services appears to be in step with Dharamsala's increased investment in its digital presence and reliance on digital systems for interacting with the increasingly global Tibetan diaspora as well as offering e-government services to Tibetan population resident in India.[9] These digital systems aim to enhance the reach and efficiency of public services, including education, social support, and other services for Tibetans, especially those residing in settlements. A universal Digital identity (Digital Green Book) is a key aspect, enabling Tibetans in the diaspora to engage with the CTA by participating in elections and accessing various services. Additionally, these systems facilitate the contribution of taxes from the diaspora, further integrating Tibetans globally into the CTA's digital governance framework.

The CTA's recognition of the importance of digital advocacy has spurred an ongoing commitment to invest in and expand its online platform presence, chief among them being www.tibet.net. This set of web resources aims to amplify the awareness of the Tibetan cause, disseminate current news and propagate awareness of its cultural heritage in Tibetan, Hindi, Mandarin and English.[10] As a result Dharamsala has become a target of cyber espionage and attacks. Agents of the PRC are constantly probing, utilising advanced techniques to undermine network security, intercept communications, and collect intelligence.[11]

One of the leaked contact lists in the dump scrutinised by Associated Press demonstrated that i-Soon scouted for databases on exiled Tibetans that they thought would sell well to the Tibetan regional government and Chinese police.[12]

II. The Cyber Threat Landscape and Attack Vectors

Historically, cyber intrusions of the CTA and Dharamsala institutions have varied from basic yet efficient phishing campaigns, like a 19-month initiative identified in 2018[13] to intricate manoeuvres such as the ExileRAT campaign of 2019.[14] The latter campaign involved a Remote Access Trojan discreetly embedded in compromised PowerPoint files, with the intention of extracting sensitive personal and organisational data. Tibetan leaders have been targeted by sophisticated WhatsApp attacks.[15] The spectrum of these cyber tactics includes masquerading as legitimate media, exploiting flaws in widely-utilised software such as Microsoft Office,[16] inserting malicious browser extensions,[17] and breaching the CTA's official internet portal.[18]

The CTA has consistently faced Advanced Persistent Threats (APTs), with the first public recognition of these security challenges occurring in 2002.[19] This predated by three years the publication of official warnings about APTs by Western intelligence services.[20] The PRC's cyber espionage activities rose to prominence among U.S. national security officials in the mid-2000s with the 'Titan Rain' cyber attacks.[21] This happened at a time when the Tibetan community abroad was increasingly turning to the internet to promote their causes and to organise their activities.

Box : 1 The Rising Complexity of Cybersecurity Threats: Advanced Persistent Threats

The advent of Advanced Persistent Threats (APTs) is a watershed moment that has reshaped our understanding of online dangers. APTs are not just random cyber incidents; they are elaborate and well-orchestrated campaigns carried out by organised groups that methodically target specific entities over long periods. This type of cyberattack is characterised by its stealth, sophistication, and strategic execution, reflecting an alarming increase in the complexity of cyber espionage activities. The battle against these threats is ongoing as security professionals strive to outpace the highly skilled adversaries behind APTs.

The Evolution and Recognition of APTs

The concept of APTs took shape in the cybersecurity community in the mid-2000s when experts began to identify a new pattern of threats. These were not hit-and-run attacks; they embodied a methodical, strategic approach that could span multiple stages, involving an array of advanced techniques to achieve their goals. One of the earliest recognized examples of APT activity was "Operation Aurora" in 2009, where major tech companies, including Google, were compromised. This attack was attributed to Chinese state-sponsored hackers who demonstrated their capabilities by using spear-phishing, exploiting zero-day vulnerabilities, and deploying backdoor malware for prolonged access.

The Proliferation of APT Incidents Over the Last Decade

Throughout the 2010s, APTs became increasingly prevalent, striking a broad range of sectors such as government, defence, and healthcare. Attackers employed progressively sophisticated and stealthy tactics that made detection and prevention extremely challenging. Illustrating the severity of these incidents, the 2015 breach of the U.S. Office of Personnel Management, again linked to Chinese operatives, and the 2017 WannaCry ransomware epidemic associated with North Korean hackers, underscored the global and high-stakes nature of APTs.

The Advanced Arsenal of APTs and Defensive Strategies

As APTs have advanced, they have embraced a more sophisticated toolset, including rootkits (software tools used to gain control over a target computer or network) and highly specialised malware that might be sourced from nation-state arsenals. Such tools are often provided by cyber “quartermasters” who supply and maintain malware, hacking groups and weapons used in support of cyber espionage operations, further complicating the threat landscape. This progression underscores the critical need for organisations to adopt forward thinking, layered cybersecurity measures. Defences must now encompass not just traditional barrier-based protection but also advanced threat intelligence and behavioural anomaly detection. Only through such comprehensive and proactive strategies can organisations and institutions like the CTA hope to counteract the severe risks posed by these targeted and relentless cyber threats.

In 2008, the "GhostNet" campaign profoundly affected the Tibetan community. This extensive cyber operation was eventually linked to a specialised division of China's military, known as Unit 61398[22] of the 3rd People's Liberation Army (3PLA). Its targets included the Private Office of the Dalai Lama located in Dharamsala, the CTA, and a range of Tibetan non-governmental organisations (NGOs). By using spear-phishing—a tactic that involves sending malware with deceptive communications designed to look legitimate—the attackers exploited software vulnerabilities to gain unauthorised access. This compromised the security and operations of the affected organisations, disrupting their crucial diplomatic engagements and advocacy work.

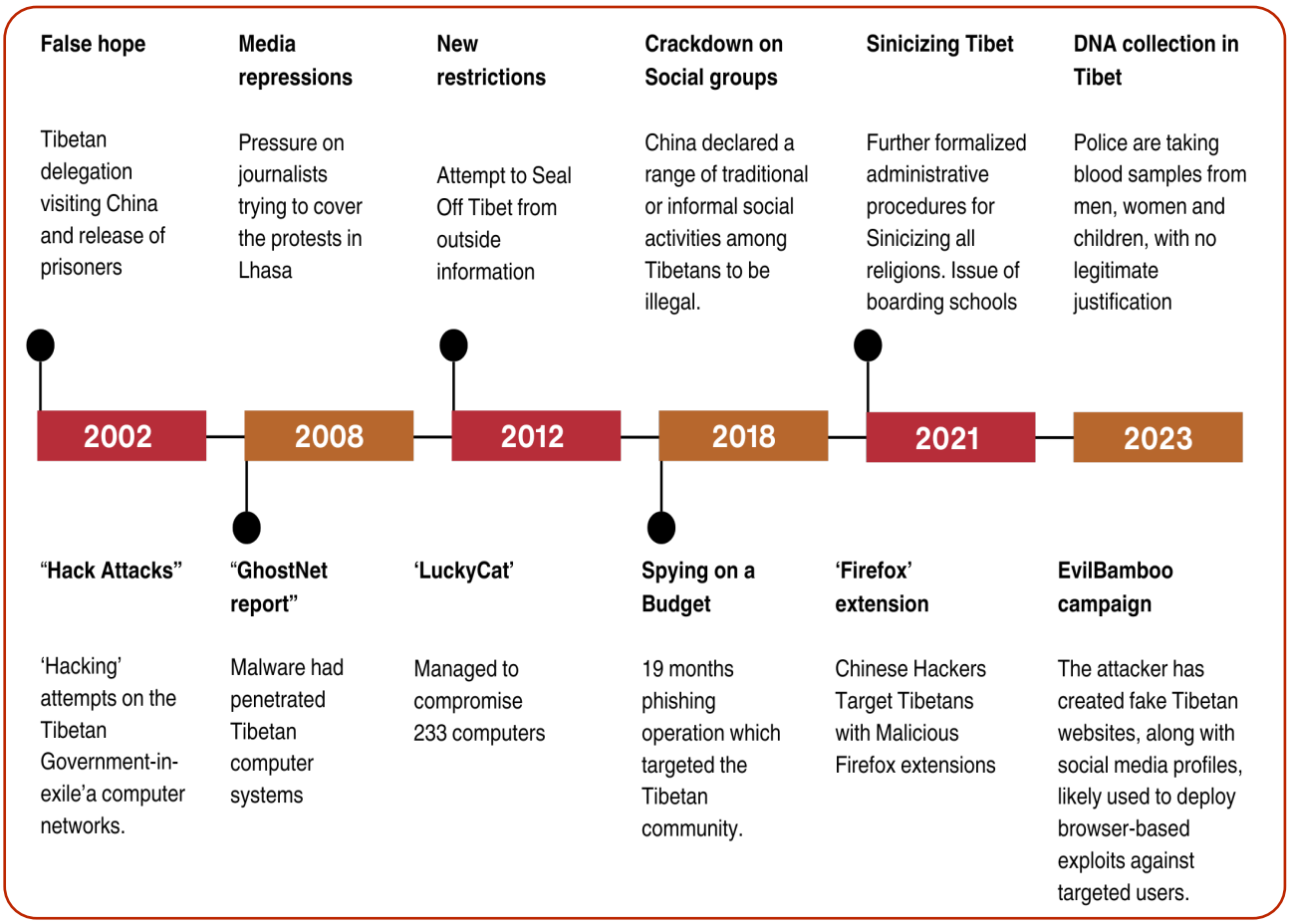


Figure 1: Chronology of Significant Offline and Cyber Incidents Impacting Tibet and the Tibetan Diaspora

The disclosure of the GhostNet campaign marked a turning point in cybersecurity. The groundbreaking report provided a clear and methodical analysis along with solid forensic evidence. It highlighted the emerging role and recognition of non-state entities in identifying and attributing cyber threats, a practice which has since become more widely accepted and valued in the cybersecurity community.[23]

Following these events, the Central Tibetan Administration (CTA) became a prime target of cyber campaigns like 'LuckyCat' in 2012[24] and 'NetTraveler,'[25] which have been linked to Chinese cyber-espionage groups. These malicious efforts targeted the CTA and various Tibetan non-governmental organisations (NGOs) internationally (for instance, the International Campaign for Tibet in the Netherlands), using seemingly relevant Tibetan-themed email attachments as a means to deliver malicious software. This malware was designed to infiltrate the computers of Tibetan activists and extract confidential data.

III. Adapting to an Evolving Cyber Threat Landscape

As the CTA invests in strengthening its digital defences, adversaries are equally enhancing their tactics. Cyber operations from China have become stealthy and sophisticated. These state-backed cyber activities are now adept at exploiting vulnerabilities, both newly discovered and previously known, with notable threat actors including Mustang Panda,[26] APT15,[27] APT21[28] APT27, TA413[29] (LuckyCat), and RedAlpha.[30] The advanced security measures they employ make their incursions hard to detect and reduce the digital evidence left behind.[31]

Data from the i-Soon leak has also been linked to previous APT campaigns targeting the CTA, the Private Office of the Dalai Lama, and Tibetan and Uyghur civil society networks. Palo Alto's Unit 42 were the first to report, with a high degree of confidence, that i-Soon are connected to an APT group known as Poison Carp.[32] [33] This attribution is based on forensic evidence surfaced in the i-Soon dump linking the company to targeting infrastructure attributed by Citizen Lab to Poison Carp[34], a Chinese threat group hitherto principally known for targeting the mobile phones of Tibetan[35] and Uyghur[36] networks. i-Soon's compromise of mobile devices would facilitate the collection of large amounts of highly sensitive information about individuals, which would put them, and those in their social network, at significant risk.

The targeting of the mobile phones of CTA officials from 2018 onwards represents a significant shift in the tactics used by threat actors, signalling an adaptation to modern communication methods and an understanding of the increasing reliance on mobile devices for both personal and professional activities.

One of the leaked contact lists in the dump scrutinised by Associated Press demonstrated that i-Soon scouted for databases on exiled Tibetans that they thought would be a particularly enticing product to the Tibetan regional government and Chinese police.[37] Indeed, operations over the past two decades to monitor and disrupt communications between the Tibetan diaspora and their compatriots in Tibet highlight the entwined nature of domestic state security and foreign intelligence operations within China. The CCP's priority of maintaining its grip on power involves extensive surveillance and control mechanisms to monitor and suppress potential internal dissent, especially when it is perceived to be connected to "hostile forces", or social movements overseas. This internal-external security nexus served as a foundation upon which broader cyber espionage activities were later developed and expanded globally.

The CTA's location in India introduces intricate challenges to its digital and physical security landscape. The persistent strain in Sino-Indian relations[38] has escalated well beyond their long-standing territorial disagreements,[39] manifesting acutely within the digital realm through acts of cyber espionage, orchestrated disinformation campaigns, and assertive digital influence tactics.[40]

In this environment, the CTA frequently becomes an unintended participant in cyber operations conducted by the People's Liberation Army (PLA), which are primarily aimed at India's security infrastructure,[41] a historical example being the PLA's 2010 "ShadowNet" campaign. This campaign was a complex ecosystem of cyber espionage primarily targeting the Indian national security establishment, but also Tibetan institutions, including the Private Office of the Dalai Lama, the CTA, and other Tibetan non-profit organisations. A report released in 2010 by the Information Warfare Monitor (a joint project of Secdev and Citizen lab) and Shadowserver Foundation detailed a sophisticated network of cyber spying that was linked back to China.[42] The investigation revealed how a vast amount of sensitive information, including personal communications of the Dalai Lama's Private Secretaries, sensitive documents related to Indian national security, and information from numerous embassies, was systematically pilfered over a period of time.

Compounding these complexities, the anticipated succession of the Dalai Lama emerges as a highly sensitive issue that draws significant scrutiny and involvement from Tibetan, Chinese, and Indian stakeholders, enmeshing the CTA even more tightly in the intricate network of regional geopolitical and security interests.

Part 2: Analysing the i-Soon Workbench and its Targeting of the CTA

A review of i-Soon's GitHub repository unearthed a trove of information, comprising over 570 distinct files directly related to the company's operations. These files reveal specialised marketing strategies for cyber espionage tools aimed at Chinese state entities. A curated selection of documents and chat transcripts within the GitHub archive has undergone examination by cybersecurity analysts. This archive is rich with technical details, such as IP addresses and infrastructural data, serving as a valuable resource for experts seeking to identify potential security breaches and the digital footprint of i-Soon's espionage technology. We have compiled an extensive bibliography that highlights the most critical studies to date in this report's annex.

Among the pivotal materials in the i-Soon data is a detailed white paper that functions as a catalogue showcasing the company's sophisticated cyber espionage tools. This white paper, titled 'Email Analysis Intelligence Decision-Making Platform,' highlights how the company's tools can be employed in cyber espionage efforts, using the Central Tibetan Administration and the digital systems employed by the Tibetan diaspora as a case study. Perhaps for the first time in the public domain, it also reveals the significant extent of their upstream analysis and (re)targeting capabilities, which enhance our understanding of the processing and utilisation of data exfiltrated by APT groups by i-Soon's Chinese intelligence and military customers.

I. The 'Email Analysis Intelligence Decision-Making Platform' (邮件分析情报决策平台) Whitepaper

The 2022 V1.0 release of the product whitepaper offers a detailed description of the functionalities of the "Email Analysis Intelligence Decision-Making Platform." Throughout the document, the compromised email inboxes of Tibetan exiles are used to demonstrate the platform's capabilities. Among the accounts featured is that of Kelsang Dorjee (Kaydor) Aukatsang. At the time of the documented intrusion into his tibet.net email,[43] Mr. Aukatsang was serving as the Chief Resilience Officer for the Central Tibetan Administration (CTA), in addition to leading the Social and Resource Development Fund (SARD).

Given his close association with the former Sikyong, Dr. Lobsang Sangay, his networks in Washington, DC policy circles, and his own candidacy for Sikyong—a position ultimately secured by Mr. Penpa Tsering—Mr. Aukatsang appears to have been identified as a high-value target within the CTA hierarchy at that time.

The introductory section of the whitepaper underscores the pivotal role of email as a conduit for a range of illicit undertakings by "cybercriminal elements". The CCP can characterise even moderate or mild views that diverge from the official Party line as "criminal". In China, email is not as widely used in everyday life as it is in most markets. The ubiquitous superapp, WeChat, is by far the most common mode of digital communication.[44] The introduction emphasises the critical importance of thorough examination of email communications as a key strategy for unearthing essential evidence and generating investigative leads. The whitepaper particularly cites email as a prime tool for '"analysis and evidence collection ... offering powerful clues in criminal cases".

It outlines the system as a "turnkey" solution, adept at providing law enforcement professionals with tools to probe and interpret comprehensive data from extensive email records, allowing them to "extract the sender and receiver email addresses, sender and receiver names, sending time, subject email body content, attachments and other information relating to the emails of interest from the massive email data obtained".

Using machine learning, the system claims to offer the capability to reveal “hidden relationships” and identify concealed patterns in the data, through social network analysis techniques.

The platform’s foremost advantage lies in its claimed capacity to process large datasets, reaching terabyte levels, which are crucial for intensifying the exploration of breached email data. The whitepaper states that the system is capable of managing “massive’’ datasets of “terabyte-scale”, catering to client requirements for scrutinising extensive email databases in “criminal investigations”. This enables decisive “rapid analysis” for mining relevant information. Investigators can initiate searches with keywords pertaining to a specific subject, subsequently extending the inquiry to the individual’s “interpersonal network” for broader insights. The system also offers “semantic analysis” to make sense of the data harvested and interpret communication patterns of the subjects under examination.

The platform supports cooperative efforts among investigative teams, allowing multiple users to annotate the compromised email database in unison. It possesses the capability to autonomously generate organisational charts centred around a particular subject of interest.

Customers have the option to utilise this robust big data analytics tool via a private cloud, which is essentially an on-premises server ensuring complete data control, or a public cloud configuration, which operates under a Software as a Service (SaaS) model, enabling access to software using external servers. The public cloud setup facilitates secure access through a two-factor authentication mechanism, complemented by a security dongle furnished by the provider, i-Soon.

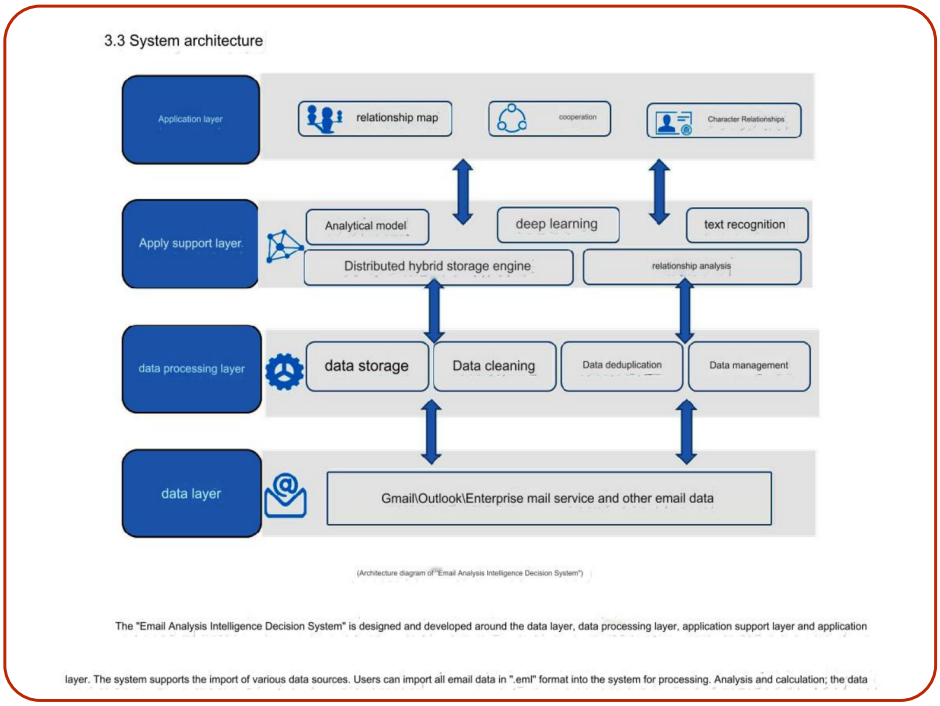


Fig. 2 System architecture diagram of the ‘Email analysis intelligence decision-making platform’ / screenshot/machine translation Source: i-Soon

Technological Architecture of the Platform

The platform's architecture is segmented into four principal layers:

1. The Data Layer: Here, the system facilitates the importation of compromised data from various sources, notably allowing for the ingestion of .eml format email files.

2. The Data Processing Layer: This stage is tasked with the analytical processing of email data, carrying out automated data cleansing, deduplication (a method of eliminating a dataset's redundant data), storage, and management.

3. The Application Support Layer: Powered by machine learning, this layer performs advanced analysis of the cleaned data, employing pre-integrated analytical models to enhance investigative interpretation.

4. The Application Layer: It supports the distributed storage system and provides an intuitive, Graphical User Interface (GUI)-based platform (a digital interface in which a user interacts with graphical components such as icons and menus) through which users navigate and interrogate the stored data via a web interface.

The system's network structure encompasses an internal Intranet, an Extranet for wider connectivity, and a secure, controlled access point demarcating the Security Boundary/ Network Access. The system proposes a Browser/Server architecture to ensure user convenience, enabling remote access at any time; however, for optimal security of sensitive data, i-Soon recommends deployment within a customer's intranet to "maintain as much isolation as possible from external networks". If external network access is necessary, the intranet system can be securely bridged to external networks through secure gateways or network proxies:

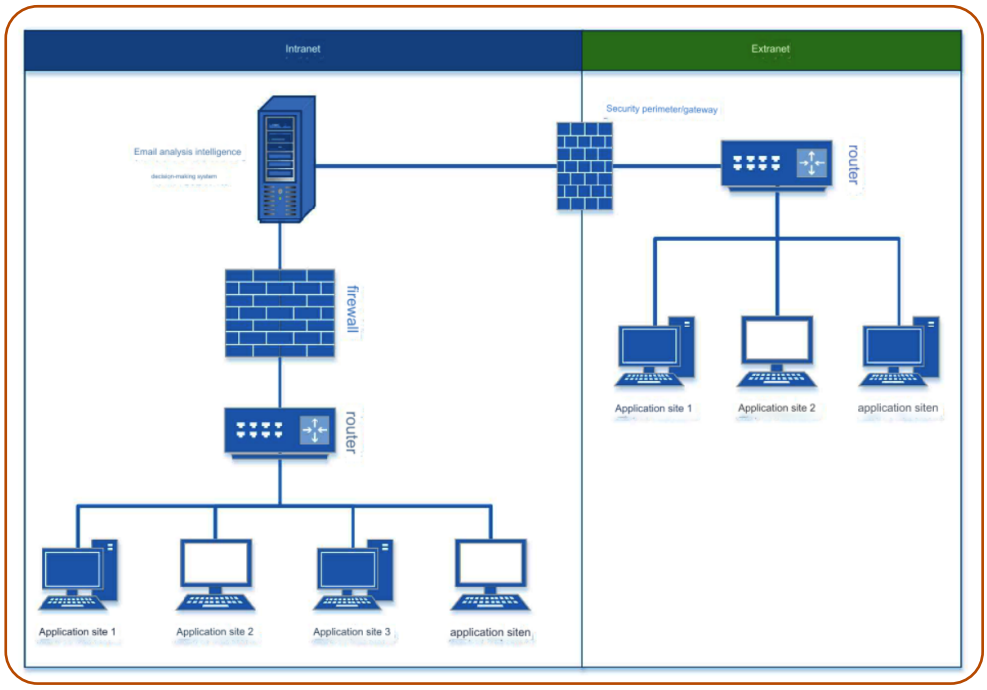


Fig. 3 Network architecture diagram of the 'Email analysis intelligence decision-making platform' / screenshot/machine translation Source: i-Soon

Functional Modules and User Interaction

1. Equipped with four essential functional modules, the platform offers:
2. Global Search and Retrieval: This module enables extensive searching throughout the dataset.
3. Mail Browsing: Users can peruse email content, effectively recreating inboxes.
4. Admin: The administrative back-end for managing users and system configurations.
5. Workbench: A comprehensive workspace for detailed analyses and the organisation of emergent findings within the visualised dataset.

The investigative process typically commences with the “Global Search” function, where specific keywords are used to swiftly gather insights from the email data. The “Workbench” interface serves as the nexus for more nuanced analysis featuring three main functions: “standard comparison analysis, single-target comparison analysis, and data snapshot”.

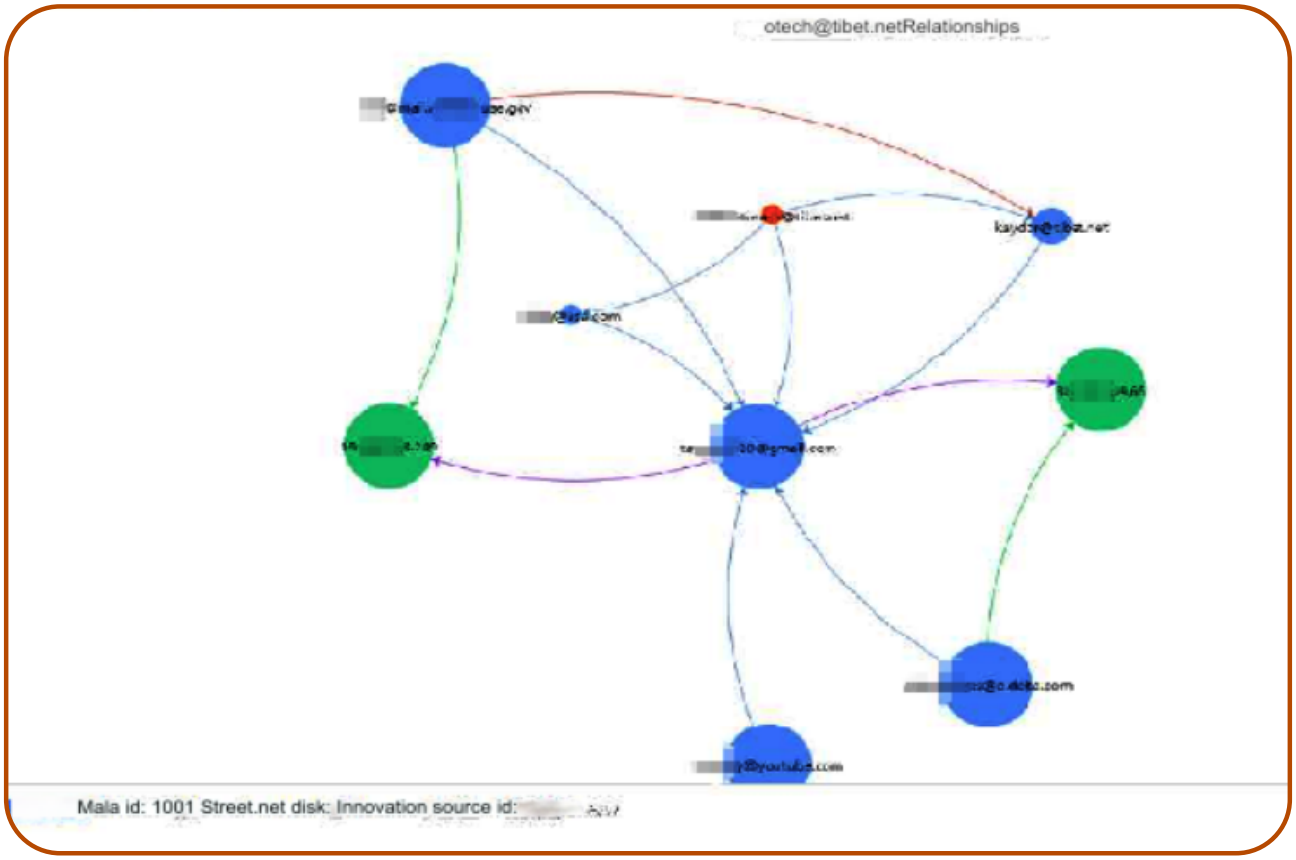


Fig. 4 The Workbench interface of the ‘Email analysis intelligence decision-making platform’ / screenshot/ machine translation showing the target otech@tibet.net and its relationship in a social graph determined by linkages in the metadata of the compromised email accounts, including kaydor@tibet.net Source: i-Soon.

Highlighted within the workbench interface imagery in the whitepaper (page 6), is the visualisation of compromised CTA email accounts which reveals the social graph and metadata linkages between these accounts, including those belonging to kaydor@tibet.net. This evidence clearly demonstrates the system's use in complex intelligence operations currently targeting the Tibetan exile community, but it is not necessarily an Indicator of Compromise.

While certain individuals or organisations may not have been directly targeted or compromised, they can still be impacted by the compromise of others within their social or organisational networks.

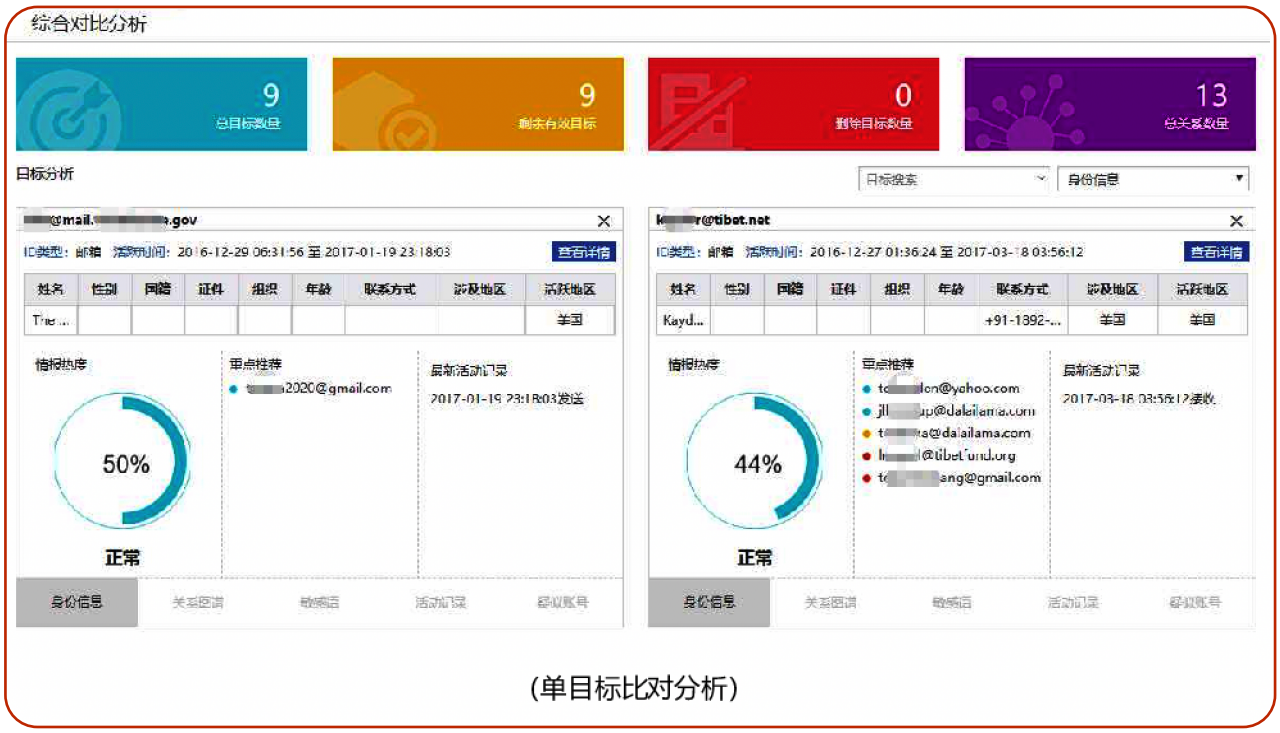


Fig. 5 The Single-Target Comparison Analysis interface of the 'Email analysis intelligence decision-making platform'. Screenshot/machine translation showing the target kaydor@tibet.net After analysing a target, the system compares information such as the target's relationship map, activity records, supporting report generation for analysis. The information for Kaydor selector shows a Dharamsala area code phone number +91-1892 [...] dated 2017-03-18 and interaction with email addresses, including correspondence with the Dalai Lama's Private Office. Source: i-Soon.

Using the term “collateral compromise” as a shorthand here captures the nuanced complexities of researching cyber espionage and digital transnational repression. For example, in the Kaydor selector (fig 5) we can see an @ dalailama.com email listed, but this does not provide us with evidence that digital infrastructure at this institution was compromised by i-Soon. In the case of the Private Office of the Dalai Lama, having their emails ingested into the Workbench without their machines being compromised, they can be considered to be “caught up” or entangled in their correspondent’s compromise. This distinction is significant and allows for a more nuanced understanding of how digital attacks can affect multiple parties indirectly.

Similarly, with regards to the Central Tibetan Administration (CTA), there may be historical indications of compromise by threat actors like Poison Carp, but the current targeting may not necessarily mean the organisation itself has been compromised. Instead, it could involve collateral compromises within their broader digital ecosystem, such as through compromised Bring Your Own Device (BYOD) policies or the compromise of correspondents in less protected NGOs or individuals in the diaspora ecosystem. Another example of this would be cases where PRC threat actors have historically targeted large mailing lists of academic experts, not by targeting the listservers themselves (which are increasingly hosted by Google), but by compromising endpoints, and thereby gaining a foothold in one node with a view to ingesting email traffic from the entire epistemic community.

By adopting the concept of collateral compromise, it becomes easier to convey the risks associated with digital transnational repression and the need to approach cybersecurity from a complex ecosystem perspective. This approach emphasises the interconnectedness of individuals and organisations within social and organisational networks, highlighting the importance of proactive measures to mitigate risks and protect sensitive information throughout the Tibetan diaspora, beyond the perimeter that TCRC monitors and defends. Ultimately, understanding and addressing collateral compromise is crucial for maintaining trust and confidence among supporters, donors, and beneficiaries, particularly when it comes to their digital communication with organisations like the CTA. It underscores the need for robust cybersecurity strategies that account for the broader ecosystemic context of digital threats and vulnerabilities.

We have reviewed the evidence demonstrating the i-Soon system's use in complex intelligence operations historically targeting the Tibetan exile community, and the use of social network analysis, for example, to analyse the interpersonal relationships of target networks of Tibetans in exile is mirrored in the intelligence methods used domestically in Tibet. A previous Turquoise Roof bulletin analysed a system description document attached to a procurement notice for the "Tibet Underworld Criminal Integrated Intelligence Application Platform", a sophisticated big data policing platform that uses social network analysis to support the investigation of "transnational organised crime".[45] This database system, which integrates other Public Security Bureau databases, and is developed on top of U.S. technology, is instrumental in a campaign that criminalises even moderate cultural, religious expressions, language rights advocacy, and crucially in the context of this bulletin, surfaces connections to exile Tibetan networks.

According to their website, i-Soon's customers include the Public Security Bureau of the Tibet Autonomous Region (西藏自治区公安厅). It is feasible that the web of interpersonal relationships surfaced from compromised inboxes of senior Tibetan civil servants in the CTA, such as those of Mr. Aukatsang, were later sold to the Public Security Bureau of the Tibet Autonomous Region and ingested into the "Tibet Underworld Criminal Integrated Intelligence Application Platform" for further social network analysis, focusing on target networks for domestic repression.

II. i-Soon's Analytical Reach: Peering into the Engine Room of State Surveillance

As the scale of the data plundered through APT operations globally became apparent in the early 2010s, researchers began to pose the question of how Chinese intelligence analysts were processing the vast datasets that they were accumulating. Strategic sense-making and meaning making, derived from Exabyte scale datasets, including structured and unstructured data, seemed to present an almost insurmountable challenge.

i-Soon's 'Email Analysis Intelligence Decision-Making Platform' shows us, at a tactical level, a crude version of some of the methods and techniques that Chinese intelligence may use to process the vast datasets that they are exfiltrating through APT operations globally. We also find the techniques used to analyse data exfiltrated from the CTA in similar tools for domestic repression.

PRC intelligence collection and analysis has been deeply influenced by the application of complex systems engineering, a multidisciplinary approach that integrates various mixed-methods techniques to 'solve' complex, real-world problems. This approach is rooted in the work of Qian Xuesen (钱学森, also known as Hsue-Shen Tsien), a prominent Chinese scientist who made significant contributions to missile and space technology, and who also laid the theoretical groundwork for systems engineering and systems science in China.[46]

Researchers have noted in recent years the foundational significance of systems engineering to the emergence of AI-driven public surveillance in China.[47] Qian's ideas have also permeated various aspects of Chinese strategic thinking and policy-making at the highest levels,[48] including intelligence collection and analysis, as evidenced, for example, by the respect accorded to his theoretical work in the preface[49] of the foundational "Sources and Techniques of Obtaining National Defence Science and Technology Intelligence".[50]

Meta-synthetic engineering plays a pivotal role in shaping intelligence analysis within China by integrating diverse streams of intelligence—ranging from quantitative data like signals intelligence to qualitative inputs such as human intelligence—into a unified analytical construct ("comprehensive" (or integrated, 综合) analysis). In theory, this sophisticated approach empowers Chinese intelligence analysts to process and interpret vast, complex datasets with increased efficiency, which in turn enhances their understanding of complex global dynamics. Such clarity is seen as essential to inform the strategic decision-making of the country's leadership. Meta-synthetic engineering has come to be seen as having transformative potential in the realm of intelligence collection and analysis.

Box 2: Understanding Meta-Synthetic Engineering in China's Intelligence Analysis

Meta-Synthetic Engineering (MSE) is an innovative interdisciplinary approach developed to tackle complex systems and issues beyond the reach of traditional scientific methods alone. Qian Xuesen pioneered it in the 1980s to overcome the limitations of conventional analytical methodologies when addressing multifaceted real-world problems.[76] MSE contrasts with Western concepts of intelligence fusion by emphasising a holistic integration of qualitative and quantitative insights, whereas the latter often focuses on data-driven analytic methods.

Unlike the Western concept of intelligence fusion that primarily deal with structured data and computational intelligence, the essence of MSE lies in its ability to progress from qualitative knowledge to quantitative wisdom from diverse disciplines — spanning natural and social sciences, engineering, and humanities — to forge a "comprehensive" understanding and derive creative solutions.[77]

The MSE method is one of participatory intelligence augmentation, relying on relatively seamless human-machine collaboration, and recognising the limitations of both human intelligence and artificial intelligence when operating in isolation, meta-synthetic engineering is an approach where teams of humans and machines work together to process and analyse information through knowledge graphs[78] and social network analysis[79], thereby leveraging the strengths of both human and machine. Given the dynamic nature of complex adaptive systems, solutions derived from meta-synthetic engineering are not static; they evolve as new information becomes available and as the system itself changes over time.

“Information Inspiritment” and its Relevance

In the late 1980s, Qian Xuesen perceived the significant potential of his developing concept of meta-synthetic engineering for intelligence gathering and analysis. This concept aimed to ‘activate’ (‘激活’) data that would otherwise remain unused.[80] This mixed-method approach is crafted to “give rise to a highly intelligent system, which not only performs the functions of collecting, storing, transmitting, retrieving, analysing, and integrating information and knowledge, but more importantly, it also generates new knowledge that can be further utilised to develop theories as well as to tackle practical issues from a holistic perspective.”[81]

Qian envisioned the activation of data through this method, which he termed ‘information inspiritment,’[82] as a cornerstone of intelligence analysis. This discipline goes beyond mere data collection; it seeks to activate the gathered data. Qian included the term ‘information inspiritment’ in his original Chinese manuscript. (He disapproved of the term ‘data fusion,’ which he also used in English, contending that it failed to fully represent the transformation of extensive dormant datasets into “live” intelligence for use in decision support systems.)[83]

III. Digital Transnational Repression: What i-Soon reveals about the objectives of China's domestic and foreign cyber operations targeting Tibetans and Uyghurs

The i-Soon archive offers researchers a significant insight into Beijing's use of complex AI-driven surveillance systems[51] to enforce political controls over Tibetan and Uyghurs, not just within its own borders, but also internationally, in the diaspora(s). The revelations shed new light on China's objectives in conducting domestic and foreign cyber operations targeting Tibetans and Uyghurs, as part of a broader strategy of transnational repression that utilises both physical and digital means to repress critics and diaspora communities. The U.S. intelligence community has recently highlighted the concerning trend of authoritarian governments increasingly using new and more intrusive technologies, including commercial spyware (surveillance) and generative artificial intelligence (disinformation), in the service of digital authoritarianism and transnational repression strategies.[52]

Authoritarian regimes are evolving their methods of surveillance and control, leveraging advancements in AI and complex systems technologies to monitor, target, and suppress dissent both domestically and abroad. In the digital realm, China is becoming more sophisticated in the use of influence operations to manipulate foreign public opinion, sway voters, shape policies, and incite social and political unrest. These operations leverage digital technologies to disseminate propaganda, misinformation, and disinformation, often through social media platforms and other online channels.

At the same time, China continues to engage in physical acts of transnational repression, including assassinations, abductions, abuse of INTERPOL Red notices, and intimidation of family members. In 2024, the Office of the Director of National Intelligence (ODNI) assessed publicly that the PRC is likely the leading perpetrator of physical transnational repression.[53] Our research over the past two decades into the targeted digital threats that Tibetan and Uyghur civil society communities face would lead us to conclude that the PRC is also the leading perpetrator of digital transnational repression.

A new report by the Tibetan Centre for Human Rights and Democracy (TCHRD) found that both physical and digital transnational repression, in which China surveils and threatens Tibetan exiles and their family and friends in Tibet, poses increasing threats to Tibetan diaspora communities.[54] TCHRD reported: "Surveillance and censorship are ubiquitous. The CCP and its proxies gather personal information on exiled Tibetans through several means: by questioning their relatives in Tibet, by exploiting cybersecurity breaches, and by mandating spies. It is important to note that the mechanisms used by the CCP to repress Tibetan activism might also be applied to wider communities, thereby constituting a threat to human rights and democracy in our societies at large."[55]

The report found various forms and trends of transnational repression experienced by exiled Tibetans worldwide including:

- United Front Work Department operatives are spying on exiled Tibetans to collect personal information that can be used to infiltrate and sabotage diaspora networks, including through disinformation campaigns, or as a basis for blackmail through hi-tech surveillance;[56]
- China is seeking to control the activities of exiled Tibetans through direct intimidation and threats to friends and family remaining in Tibet, such as coercing them into renouncing activism;
- The Chinese authorities have sought to close all avenues for Tibetans to send money to relatives in exile, leading to increased financial precarity for those seeking to establish a foothold often as refugees;[57]
- China is trying to further sever connections between Tibetans in exile and their relatives in Tibet by making communication technically impossible or dangerous.

It is on this final, critical finding that the i-Soon files provide us with fresh insights into the evolving dynamics at play, as Tibet is physically and digitally cut off from the rest of the world. Operations over the past quarter-century to monitor, later disrupt, and finally sever the communication nexus between the Tibetan diaspora and their compatriots in Tibet, highlight the intertwined nature of domestic state security and foreign intelligence operations within China. To maintain its grip on power, the CCP has developed extensive surveillance and control mechanisms to monitor and suppress potential internal dissent, especially when it is perceived to be connected to social movements overseas, characterised as "hostile forces". This internal-external security nexus may have served as a foundation upon which broader cyber espionage activities were later developed and expanded globally.

Google's Mandiant cybersecurity division has raised significant claims that Chinese intelligence services have been using diaspora populations, like Tibetan exiles, to trial new cyber attack strategies before using them worldwide.[58] This implies a systematic and calculating strategy in China's cyber activities, treating these marginalised groups as testing grounds to perfect their espionage techniques. The advantage for Chinese cyber forces and their affiliates lies in experimenting within an environment where they already have a deep understanding of the political, social, and technological context, and where the targeted networks lack strong defences. These trials serve a dual purpose: they gather intelligence on the diaspora communities and fine-tune China's capabilities in cyber warfare. This preparatory step is crucial for ensuring their tactics are more difficult to detect and attribute when used against more secure and sophisticated targets globally.

An analysis of the i-Soon leak by Wall Street Journal[59] unveiled a pattern of surveillance and cyber operations that aligns closely with the overlapping interests of the PRC security apparatuses. This reflects a broader strategy by which the Chinese government maintains its authoritarian regime through advanced technological means. The i-Soon documents revealed that the companies' customers included agencies focused on both domestic and foreign intelligence gathering, including provincial-level bureaus of China's Ministry of State Security (MSS), Ministry of Public Security (MPS), and the People's Liberation Army (PLA).[60] [61]

i-Soon's marketing of services and tools to all of these agencies, both foreign-facing and domestic, provides an insight into the depth and breadth of China's surveillance state. The company's activities in Xinjiang, where it pitched hacking capabilities to PSB officials, highlight the Chinese government's ongoing interest in surveilling and controlling the Uyghur population in that region. While its approach to selling surveillance capabilities to police in Yunnan, a region with its own diverse ethnic composition

including the Yi and Hui (Chinese Muslim) groups,[62] underscores this commercialization of state surveillance targeting China's "ethnic minority" population.[63]

This trend represents a significant evolution in how surveillance technology is deployed, suggesting that local security forces are actively seeking out advanced targeted capabilities to monitor and gather intelligence on populations deemed to be of interest or a threat. i-Soon's surveillance of minorities extended well beyond China's borders, targeting countries like Kazakhstan, Thailand, Afghanistan, and Syria, which the Wall Street Journal investigation linked to Uyghur diaspora's potential migration routes or havens.[64]

This transnational surveillance underscores China's determination to monitor Uyghur populations, wherever they are in the world. As one former Department of Defence official noted, i-Soon "were focused on domestic threats that migrated abroad. Their clients were keen on data from government bureaus, telecommunication providers, airlines, so they could monitor and access individual emails, phones."[65]

Targeting such a nexus between domestic and foreign intelligence collection is also significant in terms of our understanding of the historical origins of China's global cyber espionage programmes. It has been convincingly argued by leading APT researchers that China's cyber espionage capabilities likely originated in the early 2000s[84] from the party-state's internal security requirements:

> *"...China's cyber espionage apparatus most likely came initially out of the ruling party's own internal security needs. In addition to internal dissidents, these campaigns targeted jurisdictions that Beijing considers to be integral to the Chinese state, although it does not exercise official control over them, such as Taiwan, Hong Kong and autonomous regions in Western China. We believe that Chinese espionage operators often tested new tools and TTPs against populations in these jurisdictions before deploying them worldwide."*[85]

A quarter of a century on from these origins of APT in nascent digital transnational repression programs, through targeted malware attacks on the CTA and the diaspora(s), PRC cyber espionage by the Party state and its commercial proxies has exploded in scope and scale, to encompass the targeting of almost any internet-connected system globally. This theft of intellectual property on a post-industrial scale, where notional estimates of IP value exfiltrated by a single APT group can run into the trillions of dollars,[66] has led some experts to characterise the impact on western democracies as "theft on a scale so massive that it represents one of the largest transfers of wealth in human history."[67]

If these tactics against diaspora targets evolved directly into Beijing's global cyberespionage apparatus targeting companies and governments, then there are few more telling examples of where human rights concerns and traditional strategic priorities align than in combating the digital repression of Uyghur and Tibetan exiles.[68] Some states are beginning to actively address these threats in their policies. For example, the Transnational Repression Policy Act introduced in the U.S. Senate in 2023[69] is aimed at addressing transnational repression, including the use of commercial spyware targeting diaspora communities, through a combination of regulatory measures, sanctions, technical and psycho-social support for victims, and greater international cooperation. Its provisions are aimed at raising the costs of perpetrating repressive activities and by protecting targeted individuals and groups. At the same time, combating digital transnational repression targeting dissidents is becoming more important in the West's strategic calculus, as the U.S., for example, responds to China's cyber espionage with legal instruments. The indictment of defendants operating as part of APT31, unsealed on 25 March 2024, highlighted the group's involvement in digital transnational repression targeting Hong Kong democracy activists at the behest of the Ministry of State Security (MSS).[70]

Digital transnational repression targeting the Tibetan and Uyghur diaspora serves as a "canary in the digital coalmine" for democracies. Early warning capacity built into these digital diasporas could have surfaced these threats and led to a coordinated response in the West much sooner. Reports by Tibetan and Uyghur sources detailing digital threats from Beijing predated by several years Western intelligence's public warnings of China's cyber espionage targeting the corporate sector.

Part 3: Conclusions: The i-Soon Archive in Perspective

The i-Soon archive provides a critical window into the evolving landscape of international statecraft within the digital domain. Historically, the development of sophisticated cyber espionage capabilities was confined to government-backed laboratories and elite organisations, such as the US National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), and the extensive network of Chinese military and intelligence units. Yet, as the digital realm has seen exponential growth, it has become apparent that the traditional capacities of governments to innovate, develop cutting-edge cyber strategies, prototype systems, and allocate the significant resources these endeavours demand are being outpaced.

Commercial entities have rapidly emerged to fill the void, with expertise in open-source intelligence (OSINT), design of intricate intelligence processing systems, and the creation and refinement of malicious cyber tools—including malware. This has signalled a major shift in the landscape of digital surveillance technology, marking a departure from a time when such capabilities were the exclusive purview of state actors.[71]

In North America and Europe, proactive measures are being taken to address the complex issues arising from the vast spread of digital surveillance technologies. The United States has implemented a Presidential Directive that imposes sanctions on individuals and entities engaged in the proliferation of digital surveillance technologies that are employed in ways that deviate from lawful enforcement purposes and that encroach on human rights and civil liberties. Parallel to this, the United Kingdom and France have forged the "Pall Mall" process,[72] with similar intentions to confine and penalise the unchecked spread of such technologies.

But over the past two decades, Chinese state security's demand for overseas intelligence has increased dramatically, giving rise to a vast network of private hackers-for-hire companies such as i-Soon. According to AP's investigation, I-Soon's founder and CEO, Wu Haibo, was a member of China's first hacktivist group, Green Army — a group known informally as the "Whampoa Academy" after a famed Chinese military school.[73] Now Chinese hackers outnumber FBI cybersecurity staff by "at least 50 to one," according to an estimate by FBI director Christopher Wray.[74]

The leaked internal data offers an eye-opening and disturbing insight into the corporate strategies and motivations behind entities that market intelligence-gathering tools, and their capacity to extract and process data of valuable intelligence or security interest to their clients. For i-Soon, the marketing angle is evidenced by their targeting of specific groups—specifically the Tibetan diaspora and CTA —and by displaying their capability to infiltrate their communication systems, such as email. This serves as a showcase to attract potential clients within the Chinese intelligence and security sectors. The presence of such marketing is itself a testament to the burgeoning demand that firms like i-Soon are striving to satisfy.

Alongside usual CCP business culture norms based on the cultivation of Party connections, i-Soon also aligns itself with a national security mission. Its website claims its company culture aspires to "become a solid national defence reserve force with a strong sense of political responsibility and a spirit of high responsibility to the Party and the People."

The i-Soon archive also offers a deep dive into the corporate heartbeat of the company, providing an exhaustive compilation of internal communications, including chat logs, human resources documentation, and financial spreadsheets. This trove of information paints a vivid picture of the startup environment, highlighting the hurdles it faced in carving a niche in the market to attract a robust customer base. It also casts a revealing light on the staff's morale, flagging up issues such as dissatisfaction stemming from perceived undercompensation. The AP investigation published on 8 March noted that I-Soon executives wooed officials over lavish dinners and late night binge drinking.[75]

Implications for the CTA and a call for action

The i-Soon disclosures have concrete and far-reaching effects for the Tibetan community, particularly impacting the Tibetan diaspora and the Central Tibetan Administration. The intensifying digital dependency of marginalised populations, including Tibetans, significantly increases their exposure to cyber espionage by entities aligned with state interests and private corporations, such as i-Soon. This reality thrusts the CTA and similar non-governmental organisations into an ongoing battle to safeguard their essential digital assets. This struggle is reminiscent of an arms race, where these organisations face off against powerful state-backed and commercial entities. Lacking the shield of national sovereignty, these non-state groups encounter an even more daunting set of obstacles.

Yet, amidst these adversities lie opportunities. The CTA, in particular, can exploit the global digital infrastructure and the diverse jurisdictions where the Tibetan diaspora resides to devise defensive mechanisms that are not feasible for state actors constrained by their territorial limits.

For Tibetans and their allies, this situation serves as an urgent call to action. Ensuring the Tibetan investment in digital transformation is paralleled by a substantial commitment to securing their digital assets is imperative. Supporters of unrecognised peoples and vulnerable communities must prioritise the recognition of the perils associated with the proliferation of digital surveillance technologies. This is equally as important as providing technological assistance for these populations to advocate for their rights. Internet freedom must extend beyond the simple absence of surveillance and censorship—it must encompass a commitment to addressing the disparities in how technologies can both advance and undermine human rights.

Annex : A Note on Methodologies Used in This Report

Delving into the opaque realm of commercial cyber espionage—its mechanisms, operations, and the identities of its targets—necessitates innovative methodologies which synergistically harness the analytical prowess of social science, open-source intelligence, investigative journalism, and computer forensics to support evidence-based inquiries.

Turquoise Roof, in partnership with Western and Tibetan scholars and analysts, is committed to applying mixed-methods research. Our reports integrate diverse data types and analytical methods—encompassing personal interviews and surveys, geospatial analysis, open source intelligence and cyber forensics and investigations. This allows us to uncover new insights and construct evidence to underpin and amplify advocacy efforts.

This work builds upon a foundation laid by pioneers at SecDev and Zeropoint whose early initiatives at the University of Cambridge during the late 1990s and early 2000s were seminal in shaping the field of mixed-methods research, particularly at the confluence of conflict and information communication technologies. They were central to the establishment of both the OpenNet Initiative and the Information Warfare Monitor, and they played a pivotal role in the methodological development that supported the landmark GhostNet investigation, which exposed cyber espionage targeting the offices of His Holiness the Dalai Lama in 2008.

In the pursuit of understanding complex issues at the intersection of technology and human rights, we employ methods spanning social science, investigative journalism, computer forensics, and open-source intelligence.

Groundbreaking projects like the OpenNet Initiative and the Information Warfare Monitor required not only a comprehensive understanding of computer technology but also the adoption of novel data collection techniques. One such technique involves the analysis of extensive data sets or ‘data dumps’, which have, for instance, propelled the investigation covered in this report concerning the activities of i-Soon.

Central to the investigative process is the active use of technical tools for empirical verification. This includes probing to ascertain the veracity of claims surrounding surveillance or censorship. Through rigorous examination, documented evidence of these practices becomes indisputable. Such investigative research is increasingly vital. Communities like the Tibetan diaspora are recognizing the value of embracing these methods, not only for generating new data but also for corroborating evidence related to incidents of digital surveillance as documented within this report.

It is important to note that mixed-methods research is still a relatively nascent field, one that is undergoing rapid evolution. The advent of artificial intelligence, which facilitates quicker development of data collection platforms and enhances the capacity for data processing and analytical rigour, is poised to significantly influence and expedite the maturity of these investigative techniques.

Turquoise Roof aims to apply and hone these techniques in investigations such as this report, while also integrating the expertise and insights of Tibetan researchers and Tibet watchers, enabling us to derive fresh insights and forge robust evidence that can strengthen advocacy efforts.

Bibliography

The original GitHub repository was located at: https://github.com/I-S00N/I-S00N

Published on 16 February, 2024. On 23 February, 2024 it was disabled as it was reportedly "found to be in violation of GitHub's Acceptable Use Policies on doxxing and invasion of privacy."

'Major Chinese hack' on Foreign Office urgently investigated by UK spies (The Independent)

Richard Holmes, Sanya Burgess

February 20, 2024 5:46 pm (Updated February 21, 2024 10:44 am)

https://inews.co.uk/news/spies-chinese-hack-foreign-office-2916594

Anonymous dump of internal files said to be from a Shanghai-based surveillance company shows a list of targets in Whitehall, including the Foreign & Commonwealth Office

Unmasking I-Soon I The Leak That Revealed China's Cyber Operations (Sentinel One)

Dakota Cary and Aleksandar Milenkoski

February 21, 2024

https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/

Leaked files from Chinese firm show vast international hacking effort (Washington Post)

Christian Shepherd, Cate Cadell, Ellen Nakashima, Joseph Menn and Aaron Schaffer

Updated February 22, 2024 at 10:01 a.m. ESTIPublished February 21, 2024 at 8:00 p.m. EST

https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-i-Soon/

This reporting includes a reference sourced from an i-Soon chat transcript that mentions possession of credentials for a CTA network.

Lessons from the i-Soon Leaks (@BushidoToken Threat Intel)

https://blog.bushidotoken.net/2024/02/lessons-from-i-Soon-leaks.html February 22, 2024

Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns (Unit 42, Palo Alto Networks)

https://unit42.paloaltonetworks.com/i-soon-data-leaks/ l日本語 (Japanese) version: https://unit42.paloaltonetworks.jp/i-soon-data-leaks/

February 23, 2024 at 5:00 PM (PT)

- This reporting surfaces an IP address in the i-Soon archive that Citizen Lab attributed to a group targeting Tibetans in 2019, that they track as Poison Carp. (Volexity as Evil Bamboo.)

Leaked Hacking Documents Show China's Focus on Tracking Ethnic Minorities (WSJ)

Liza Lin and Asutin Ramzy

Feb. 26, 2024 11:00 pm ET

https://www.wsj.com/world/china/china-hacking-documents-target-ethnic-minorities-1c582813

i-SOON: Kicking off the Year of the Dragon with Good Luck … or Not (NATTO TEAM)

Chat logs in the i-SOON leak show China's hacker-for-hire industry is subject to Chinese business culture: in the race for profits, survival depends on who you know and who you dine and wine with.

28 Feb 2024

https://nattothoughts.substack.com/p/i-soon-kicking-off-the-year-of-the

Same Same, but Different (Margin Research)

Winnona Bernsen

Feb 29, 2024

https://margin.re/2024/02/same-same-but-different/

A Comprehensive Analysis of i-Soon's Commercial Offering (Harfang Lab)

1 March, 2024

https://harfanglab.io/en/insidethelab/i-Soon-leak-analysis/

Attributing I-SOON: Private Contractor Linked to Multiple Chinese State-sponsored Groups (Insikt Group®)

20 March 2024

https://www.recordedfuture.com/attributing-i-soon-private-contractor-linked-chinese-state-sponsored-groups

Endnotes

1 Unit 42 (2024) Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns, Palo Alto Networks, February 23, https://unit42.paloaltonetworks.com/i-soon-data-leaks/

2 Marczak, B., Hulcoop, A., Maynier, E., Abdul Razzak, B., Crete-Nishihata, M., Scott-Railton, J., and Deibert, R. (2019) Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits, The Citizen Lab, 24 September, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

3 Roxan, C., Rascagneres, P., and Lancaster, T. (2023) EvilBamboo Targets Mobile Devices in Multi-year Campaign (Volexity). September 22, 2023

https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-mobile-devices-in-multi-year-campaign/

[Ed: formerly tracked by Volexity as Evil Eye, which Citizen Lab later designated Poison Carp. See also Ian Beer (2019) Project Zero, Google, August 29, https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html]

4 Case, A., Meltzer, M., and Adair, S. (2019) Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs, Volexity, September 2, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

5 Chin, J and Lin, L. (2022) The American-Trained Rocket Scientist Who Shaped China's Surveillance System

(An Excerpt from 'Surveillance State: Inside China's Quest to Launch a New Era of Social Control'). China File, September 6, https://www.chinafile.com/library/excerpts/american-trained-rocket-scientist-who-shaped-chinas-surveillance-system

6 Developers in China widely use GitHub for both open-source projects and commercial software development, making it a critical resource in the country's tech industry. The platform has been blocked in the past, most notably in 2013 and briefly in 2015, usually due to the hosting of content or tools designed to circumvent internet censorship, or content considered politically sensitive by the Chinese government. However, given the importance of GitHub for software development and innovation, complete and sustained blocks have proven challenging and potentially detrimental to China's own technological and economic interests. As a result, the Chinese government has at times taken a more nuanced approach, potentially targeting specific repositories or content rather than imposing a full platform-wide block.

7 The SecDev Group (2009) Tracking GhostNet: Investigating a Cyber Espionage Network, March 29, https://www.secdev.com/Whitepapers/Tracking+Ghostnet.pdf

8 McConnell, F. (2016) Rehearsing the state: The political practices of the Tibetan government-in-exile, John Wiley & Sons, https://www.stcatz.ox.ac.uk/publications/rehearsing-the-state/

9 CTA convenes first-ever Digital Strategy Development Meeting, October 20, 2022 https://tibet.net/cta-convenes-first-ever-digital-strategy-development-meeting/

10 www.tibet.net

11 Kaiman, J. (2013) Hack Tibet: Welcome to Dharamsala, ground zero in China's cyberwar, Central Tibetan Administration, 5 December, https://tibet.net/hack-tibet-welcome-to-dharamsala-ground-zero-in-chinas-cyberwar/.

12 Kang, D. and Soo, Z. (2024) Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex, AP, March 8,

https://apnews.com/article/chinese-hacking-leak-documents-surveillance-spying-6276e8662ddf6f2c1afbae994d8b3aa2

13 Crete-Nishihata, M., Dalek, J., Maynier, E., and Scott-Railton, J. (2018) Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community, The Citizen Lab, 30 January, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/

14 Osborne, C. (2019) Pro-Tibet groups targeted with ExileRAT in spy campaign, ZDNet, 5 February, https://www.zdnet.com/article/pro-tibet-groups-targeted-with-exilerat-in-spam-campaign/

15 Marczak, B., Hulcoop, A., Maynier, E., Abdul Razzak, B., Crete-Nishihata, M., Scott-Railton, J., and Deibert, R. (2019) Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits, The Citizen Lab, 24 September, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

16 Faife, C. (2022) China-linked hackers are exploiting a new vulnerability in Microsoft Office, The Verge, June 1, https://www.theverge.com/2022/6/1/23150318/microsoft-office-china-hackers-exploiting-follina-vulnerability-tibet. Central Tibetan Administration (n.d.) News, Official Chinese Website of the Central Tibetan Administration, https://xizang-zhiye.org

17 Muncaster, P. (2021) Chinese hackers target Tibetans with malicious Firefox extension, Infosecurity Magazine, 26 February, https://www.infosecurity-magazine.com/news/chinese-hackers-tibet-malicious/

18 AP (2013) Tibetan government-in-exile's site hit by hackers, 13 August, https://apnews.com/general-news-1c90ee53bd-1b494587ae6ba70abb8c85

19 Nairne, D. (2002) State hackers spying on us, say dissidents, South China Morning Post, 18 September, https://archive.is/EPjlS#selection-815.13-861.32

20 Batty, D. (2005) Hackers target vital UK IT networks, The Guardian, 16 June, https://www.theguardian.com/society/2005/jun/16/epublic.politics

21 Council on Foreign Relations (2005) Cyber Operations: Titan Rain, August, https://www.cfr.org/cyber-operations/titan-rain

22 Council on Foreign Relations (n.d.) Cyber Operations: PLA Unit 61398, https://www.cfr.org/cyber-operations/pla-unit-61398

23 Council on Foreign Relations (n.d.) Cyber Operations: GhostNet, https://www.cfr.

org/cyber-operations/ghostnet.

24 Forward-Looking Threat Research Team (2012). LUCKYCAT REDUX: Inside an APT Campaign with Multiple Targets in India and Japan, Trend Micro, https://web.archive.org/web/20120331144944/http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf

25 Raiu, C. (2013) NetTraveler is back: the 'Red Star' APT returns with new tricks, Securelist, September 3, https://securelist.com/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/57455/

26 Cybalt (2023) Chinese hacking group, Mustang Panda exploiting TP-Link firmware, LinkedIn, June 27, https://www.linkedin.com/company/cybalt?trk=article-ssr-frontend-pulse_publisher-author-card

27 U.S.-China Economic and Security Review Commission (2022), China's cyber capabilities: Warfare, espionage, and implications for the United States, https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf

28 Rosengren, O. (2023) APT networks: A force multiplier in China's push for global power, Grey Dynamics, May 9, https://greydynamics.com/apt-networks-a-force-multiplier-in-chinas-push-for-global-power/

29 Raggi, M. and the Proofpoint Threat Research Team (2020) Chinese APT TA413 resumes targeting of Tibet following COVID-19 themed economic espionage campaign delivering sepulcher malware targeting Europe, Proofpoint, September 1, https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

30 The Hague Centre for Strategic Studies (2022) Cyber Arms Watch: An analysis of stated & perceived offensive cyber capabilities, May 2022, https://hcss.nl/wp-content/uploads/2022/05/Cyber-Arms-Watch-HCSS-2022-1.pdf.

31 Insikt Group (2023). Charting China's climb as a leading global cyber power, Recorded Future, November 7, https://go.recordedfuture.com/hubfs/reports/cta-2023-1107.pdf

32 Unit 42 (2024) Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns, Palo Alto Networks, February 23, https://unit42.paloaltonetworks.com/i-soon-data-leaks/

33 RecordedFuture's Insikt Group corroborated these links in a report published on 20 March, 2024 and identified additional overlaps between POISON CARP-linked infrastructure and i-Soon: https://www.recordedfuture.com/attributing-i-soon-private-contractor-linked-chinese-state-sponsored-groups

Insikt Group attributed further Chinese threat activity groups linked to iSoon, including RedAlpha - a group that orchestrated APT campaigns targeting the Tibetan community that took place in 2017 and 2018, see https://www.recordedfuture.com/blog/redalpha-cyber-campaigns (28 June, 2018)

34 Marczak, B., Hulcoop, A., Maynier, E., Abdul Razzak, B., Crete-Nishihata, M., Scott-Railton, J., and Deibert, R. (2019) Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits, The Citizen Lab, 24 September, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-

exploits/

35 Roxan, C., Rascagneres, P., and Lancaster, T. (2023) EvilBamboo Targets Mobile Devices in Multi-year Campaign (Volexity). September 22, 2023

https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-mobile-devices-in-multi-year-campaign/

[Ed: formerly tracked by Volexity as Evil Eye, which Citizen Lab later designated Poison Carp. See also Ian Beer (2019) Project Zero, Google, August 29, https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html]

36 Case, A., Meltzer, M., and Adair, S. (2019) Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs, Volexity, September 2, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

37 Kang, D. and Soo, Z. (2024) Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex, AP, March 8,

https://apnews.com/article/chinese-hacking-leak-documents-surveillance-spying-6276e8662ddf6f2c1afbae994d8b3aa2

38 Markey, D., and Scobell, A., (2023) Three Things to Know About China-India Tensions, United States Institute of Peace, October 19, https://www.usip.org/publications/2023/10/three-things-know-about-china-india-tensions

39 The number of Chinese border incursions into Himalayan territory has tripled since Xi Jinping took charge, according to a dataset presented in the International Crisis Group report. See International Crisis Group (2023) Thin Ice in the Himalayas: Handling the India-China Border Dispute, Asia Report no 334, November 14, https://www.crisisgroup.org/asia/south-asia/india-china/334-thin-ice-himalayas-handling-india-china-border-dispute

40 Kurlantzick, J. (2023) China's Influence Activities in India, Council on Foreign Relations, February 13, https://www.cfr.org/blog/chinas-influence-activities-india.

41 Robertson, G. (2010) Spies reach deep into India's defence, The Globe and Mail, April 6,

https://www.theglobeandmail.com/technology/spies-reach-deep-into-indias-defence/article4188949/

42 Information Warfare Monitor and Shadowserver Foundation (2010) Shadows in the Cloud, SecDev, April 6, https://www.secdev.com/Whitepapers/shadows-in-the-cloud.pdf

43 2016-12-27 01:36:24 to 2017-01-19-23 06:31:56

44 Liang, L.-H. (2020) Why email loses out to popular apps in China, BBC, July 9, https://www.bbc.com/worklife/article/20200707-why-email-loses-out-to-popular-apps-in-china

45 Turquoise Roof (2024) Weaponizing Big Data: Decoding China's Digital Surveillance In Tibet, Turquoise Roof Briefings No.3, February 7, https://turquoiseroof.org/weaponising-big-data-decoding-chinas-digital-surveillance-in-tibet/

46 Science/AAAS Custom Publishing Office (2016) The rise of systems engineering in China, September 27,

https://www.science.org/content/resource/rise-systems-engineering-china

47 Hvistendahl, M, (2018) A revered rocket scientist set in motion China's mass surveillance of its citizens, Science, March 14, https://www.science.org/content/article/revered-rocket-scientist-set-motion-china-s-mass-surveillance-its-citizens; Chin, J, Lin, L. The American-Trained Rocket Scientist Who Shaped China's Surveillance System

(An Excerpt from 'Surveillance State: Inside China's Quest to Launch a New Era of Social Control') September 6, 2022 https://www.chinafile.com/library/excerpts/american-trained-rocket-scientist-who-shaped-chinas-surveillance-system

48 Stone, A. (2024) "A Complex Systems Engineering Undertaking" The Qian Xuesen School Of Systems Engineering: BluePath Labs Report, China Aerospace Studies Institute, ed. Dr. Eric Hundman, February 2024 https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Infrastructure/2024-02-20%20Complex%20Systems%20Engineering.pdf

49 "Professor Qian Xuesen gave an important speech at the National Defence S&T Intelligence Working Conference in July of 1983. His topic was: "I Maintain that the Matter of Information Collection is a Science and a Technology and We Should Put Forth Our Best Efforts to Research Information Collection." The words of Professor Qian Xuesen moved us deeply. Firstly, because we had learned from the experience of actual information collection work that, while information collection appears simple, it is by no means an easy matter to do it well, for the subject embraces many "mysteries." Secondly, Professor Qian's words moved us because, although we and many of our comrades who were engaging in information collection had already accumulated a considerable amount of practical experience in our particular posts of duty, we had not by any means elevated these practical experiences to the theoretical level. One might say that our information collection still lacked the necessary theoretical guidance, with the result that it was still mired in a state of affairs characterised by "routinism," the consideration of matters in and of themselves, and virtually complete blindness. The facts prove that the direction that Professor Qian Xuesen pointed out--putting forth efforts to research information collection learning, and establishing theory (the science of information collection) to guide information collection work--is a job that cannot be shirked by intelligence personnel." See ZhongWen, H. and Zongxiao, W. (1991) Sources and Techniques of Obtaining National Defense Science and Technology Intelligence: Preface, Federation of American Scientists: Intelligence Resource Program, https://irp.fas.org/world/china/docs/sources_pref.html

50 霍忠文, 王宗孝 (1991) 国防科技情报源及获取技术 (available in translation see ZhongWen, H. and Zongxiao, W. (1991) Sources and Techniques of Obtaining National Defense Science and Technology Intelligence: Preface, Federation of American Scientists: Intelligence Resource Program, https://irp.fas.org/world/china/docs/sources.

html)

51 Chin, J and Lin, L. (2022) The American-Trained Rocket Scientist Who Shaped China's Surveillance System

(An Excerpt from 'Surveillance State: Inside China's Quest to Launch a New Era of Social Control'). China File, September 6, https://www.chinafile.com/library/excerpts/american-trained-rocket-scientist-who-shaped-chinas-surveillance-system

52 Office of the Director of National Intelligence (2024) Annual Threat Assessment of the U.S. Intelligence Community,

p 31, February 5, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

53 ibid., p.31

54 Tibetan Centre for Human Rights and Democracy (TCHRD) (2024): Report reveals Chinese Transnational Repression spreading fear and disempowering exiled Tibetans, February 5, https://tchrd.org/report-reveals-chinese-transnational-repression-spreading-fear-and-disempowering-exiled-tibetans/

55 ibid.

56 A Tibetan in Belgium told TCHRD: "[At a protest outside the Chinese Embassy in Brussels] there are also some high-tech rotating cameras, used to take images of Tibetan protesters who would then be refused visas if they ever applied to visit their families in Tibet. It's a similar situation at the Chinese embassy in the Netherlands."

57 TCHRD states: "Going into exile tends to entail a stage of economic precarity - the cost of organising one's border crossing and journey to a safe destination, but also the administrative and living costs when settling into a new country where one may not have the right to work immediately. For this reason, while they wait for their new situation to stabilise, exiled Tibetans often rely on money sent by their relatives back in Tibet. By closing this avenue, Chinese authorities seek to impoverish and disempower exiled Tibetans."

58 Mandiant 2019, p.29 or the M-Trends 2019 report

59 Lin, L., and Ramzy, A. (2024) Leaked Hacking Documents Show China's Focus on Tracking Ethnic Minorities, TheWall Street Journal, February 26,

https://www.wsj.com/world/china/china-hacking-documents-target-ethnic-minorities-1c582813

60 Ibid.

61 Lin, L. (2024) 9/ China's APTs tend to go after military and IP intelligence, X, February 27, https://twitter.com/lizalinwsj/status/1762429214664409598

62 Lin, L. (2024) 2/ We analyzed victims and noticed they had something in common, X, February 27, https://twitter.com/lizalinwsj/status/1762424573255926245

63 The PRC officially recognizes 55 'ethnic minority' groups in addition to the Han Chinese majority. However, the very definition of 'ethnic minorities' or 'nationalities' in the PRC has been conceived by the state and does not reflect the self-identification of Tibetans, Uyghurs, or others who fall under this category - nor does the term convey the complex

realities of their culture and history.

64 Lin, L. (2024) 3/ In one proposal, I-Soon dangled access to what it termed “anti-terrorist” data, X, February 27, https://twitter.com/lizalinwsj/status/1762425264103989746

65 Lin, L. (2024) 7/ Great observation by @TangAnZhu, X, February 27, https://twitter.com/lizalinwsj/status/1762427437671940386

66 Cybereason Nocturnus (n.d.) Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation, https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation

67 Wray, C. (2020) The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States: Remarks as delivered, Hudson Institute, July 7, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

68 Gottlieb, A. and Christine, B. (2022) The Big Question: How Has Beijing Suppressed And Influenced International Responses To Its Repression Of Uyghurs In China And Abroad? National Endowment for Democracy, September 28, https://www.ned.org/the-big-question-how-has-beijing-suppressed-and-influenced-international-responses-to-its-repression-of-uyghurs-in-china-and-abroad/ (Remarks by Greg Walton, SecDev Group)

69 US Congress (2023) Summary: S.831 — 118th Congress (2023-2024) https://www.congress.gov/bill/118th-congress/senate-bill/831

70 U.S. Attorney’s Office, Eastern District of New York, Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians

Monday, March 25, 2024 https://www.justice.gov/usao-edny/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting

71 Research organisations including Citizen Lab and Amnesty International have revealed the emergence of private cyber espionage firms like i-Soon. Their findings highlight a troubling trend where companies such as NSO Group of Israel distribute spyware technology that empowers repressive regimes. This contributes to a growing global wave of digital authoritarianism, where state surveillance and control are enhanced through advanced technology.

72 UK and France (2024) Pall Mall Process on proliferation and irresponsible use of commercial cyber intrusion capabilities: UK and France joint communiqué, Government of UK, February 7, https://www.gov.uk/government/publications/pall-mall-process-on-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities-uk-and-france-joint-communique

73 Kang, D. and Soo, Z. (2024) Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex, AP, March 8,

https://apnews.com/article/chinese-hacking-leak-documents-surveillance-spy-

ing-6276e8662ddf6f2c1afbae994d8b3aa2

74 Rabinowitz, H. and Lyngaas, S. (2024) FBI director warns that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure, CNN, January 31, https://edition.cnn.com/2024/01/31/politics/china-hacking-infrascture-fbi-director-christopher-wray/index.html

75 Cybersecurity analyst Mei Danowski is cited by AP (8 March 2024) as saying: "It is subject to China's business culture — who you know, who you dine and wine with, and who you are friends with." Mei Danowski cites from the i-Soon website on her blog, Kang, D. and Soo, Z. (2024) Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex, AP, March 8,

https://apnews.com/article/chinese-hacking-leak-documents-surveillance-spying-6276e8662ddf6f2c1afbae994d8b3aa2, see also Natto team (2023) i-SOON: Another Company in the APT41 Network, Natto Thoughts, October 26, https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41

76 Science/AAAS Custom Publishing Office (2016) The rise of systems engineering in China, September 27,

https://www.science.org/content/resource/rise-systems-engineering-china

77 ibid.

78 Ren, M., Chen, N. and Qiu, H. (2023) Human-machine Collaborative Decision-making: An Evolutionary Roadmap Based on Cognitive Intelligence. Int J of Soc Robotics 15, 1101–1114, https://doi.org/10.1007/s12369-023-01020-1

79 Tang, X., (2007) Towards meta-synthetic support to understand unstructured problem solving. International Journal of Information Technology & Decision Making Vol. 06, No. 03, pp. 491-508, https://doi.org/10.1142/S0219622007002630

80 Stone, A. (2024) "A Complex Systems Engineering Undertaking" The Qian Xuesen School Of Systems Engineering: BluePath Labs Report, China Aerospace Studies Institute, ed. Dr. Eric Hundman, February 2024 https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Infrastructure/2024-02-20%20Complex%20Systems%20Engineering.pdf

81 ibid. p. 34

82 ibid. p. 35

83 ibid. p. 35, see footnote xxxi

84 Nairne, D. (2002) State hackers spying on us, say dissidents, South China Morning Post, September 18, https://archive.is/EPjlS#selection-815.13-861.32.

85 Mandiant 2019, p.29 of the M-Trends 2019 report


TURQUOISE
ROOF