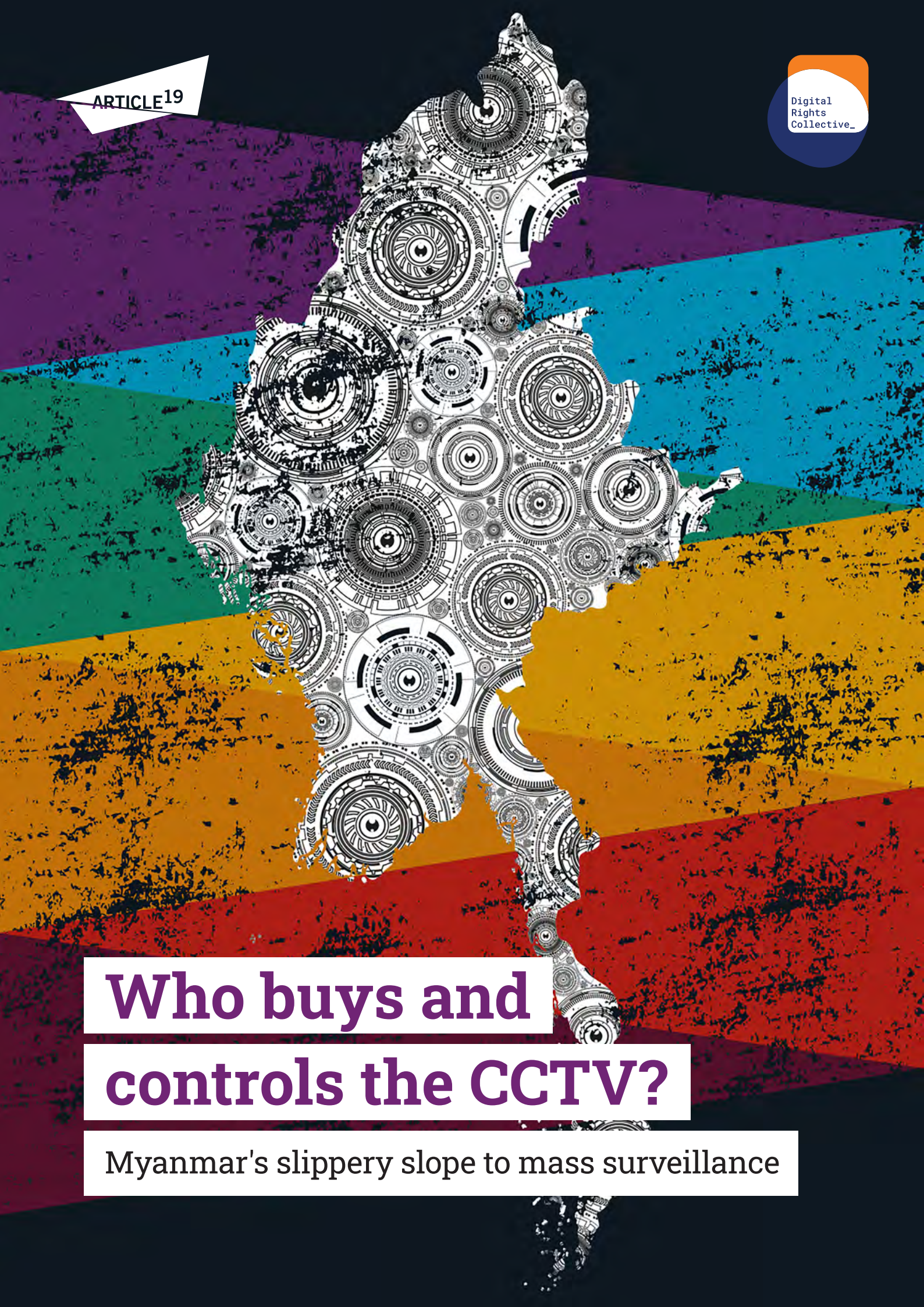


ARTICLE 19

Digital Rights Collective_

Who buys and controls the CCTV?

Myanmar's slippery slope to mass surveillance

First published by ARTICLE 19, August 2022

ARTICLE 19

www.article19.org

A19/DIG/2022/001

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas, and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by power-holders for transparency, good governance, and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

Digital Rights Collective is an organisation with a group of activists, researchers and civic tech enthusiasts working to further digital rights in Myanmar. Digital Rights Collective aims to create an empowered community for Myanmar, collectively furthering rights on the Internet through safe space and progressively solving issues through innovations.

Acknowledgements

ARTICLE 19 and Digital Rights Collective are grateful to **Dr Matt Mahmoudi** and **Shazeda Ahmed** for their valuable feedback on earlier drafts of this report. We also wish to thank our civil society interviewees for their time and insightful comments.

If you would like to discuss any aspect of this report further, please email **info@article19.org** or **info@digitalrightsco.org**

Contents

Abbreviations

AI	Artificial intelligence
ASCN	ASEAN Smart Cities Network
ASEAN	Association of Southeast Asian Nations
CCTV	Closed-circuit televisions
ICCPR	International Covenant on Civil and Political Rights
MCDC	Mandalay City Development Committee
NLD	National League for Democracy
UDHR	Universal Declaration of Human Rights

Executive summary

In this report, **ARTICLE 19** and **Digital Rights Collective** investigate how closed-circuit televisions (CCTV) are procured in Myanmar.

An underlying concern for this report is the transparency of public procurement and spending and accountability of government operations. Public procurement is supposed to provide for citizens' needs, and therefore it must be accountable to the public. Access to information is key to this accountability. Transparency of public procurement allows civil society to act as an effective watchdog on government systems, making recommendations for change and bringing this crucial area – where public and private sectors meet – under better public scrutiny.

CCTV cameras form an essential prerequisite for artificial intelligence (AI)-based biometric surveillance technologies that make up smart cities' infrastructure, such as live and retrospective facial recognition, automated number plate recognition, and emotion recognition, among others. Given the grave human rights implications of CCTV infrastructure and its increasing scale in the country, we seek to understand the compounding risks of this technology against the backdrop of a military coup. This is crucial to study, given that CCTVs are an important building block for remote biometric identification and mass surveillance, both of which are steadily becoming entrenched across Myanmar.

Thousands participate in a protest against the military coup in Yangon's downtown area, Sule. CCTV cameras are installed on all four sides of the Sule junction.
Photo: February 2021, Digital Rights Collective.

Our report demonstrates how CCTVs are procured and deployed in Myanmar, and the human rights implications of their use. It aims to:

1. Equip civil society with the necessary background and context on public procurement within the country to carry out further research and advocacy;
2. Provide relevant context of Myanmar's political reality, legal framework, and legacy of surveillance;
3. Outline key information on current technologies of interest and entities building and supplying these technologies;
4. Analyse the human rights implications of CCTV systems; and
5. Highlight areas of further investigation.

In particular, this report emphasises the dire need for transparency and accountability within the country's procurement processes and technology deployment. We seek to highlight that studying traditional infrastructures like CCTV is important for digital rights activists and academics as it is these infrastructures that pave the way for 'smart' biometric technologies to scale rapidly further down the line in the absence of legislation, safeguards, oversight, or human rights considerations.

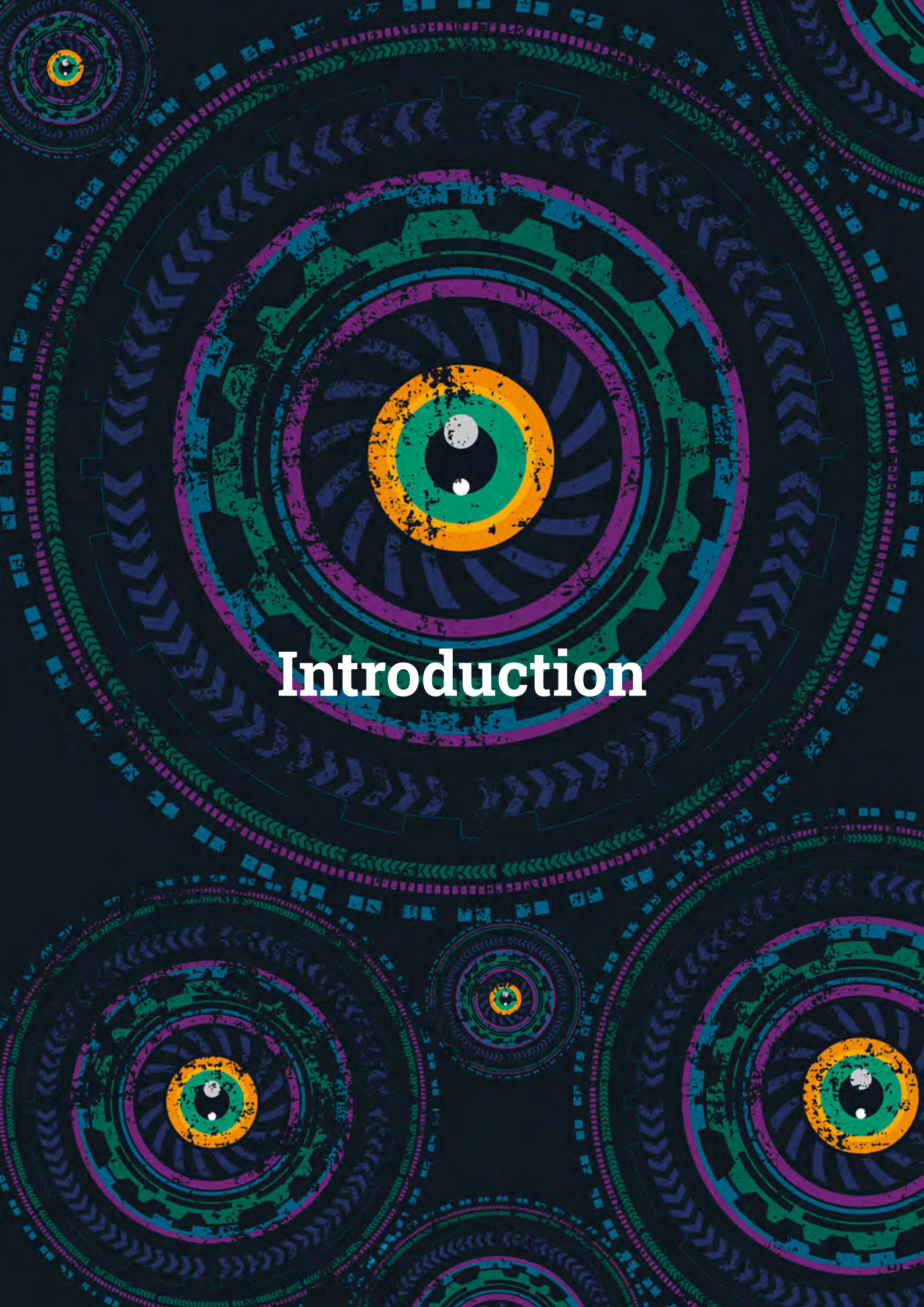
In the pages that follow, we trace how CCTV cameras came to be normalised and adopted within three cities in Myanmar, namely Mandalay, Yangon, and

Naypyidaw. We investigate who is building CCTV technology, who buys such technology, the purported use cases intended for these technologies, and their resulting implications against the backdrop of a military coup. The findings presented here are useful to civil society actors for thinking through the potential harms arising from the use of CCTV cameras and subsequent AI applications in Myanmar and beyond, particularly in jurisdictions where similar crises are likely to happen. With information gathered from media reports, government tenders, leaked government documents, and interviews conducted before the military coup, we discuss how smart city technologies are currently procured in Myanmar to highlight a crucial stage of smart city deployment that civil society is rarely able to influence. We also analyse the impact of such technologies on human rights, particularly freedom of expression, privacy, and freedom of peaceful assembly, and demonstrate the need for a more rigorous analysis of the potential impact of technical infrastructure from the stage of procurement to deployment. Finally, we draw attention to the lack of transparency and the pieces of information that are not known to us to highlight the difficulty and secrecy of the working of the government's infrastructure. Overarchingly, we point to how opacity is normalised as a feature and not a bug within Myanmar's technology procurement framework and we provide recommendations for a way forward.

In this report, we lay down the essential components of a rights-respecting framework for developing smart cities in Myanmar, and make recommendations to the military junta in Myanmar, and to the private sector. The military junta should stop purchasing, developing, and using technologies, particularly emotion recognition technologies, that impact human rights. The private sector should stop selling and deploying equipment for smart city infrastructures to authoritarian dictatorships. They should also ensure that the design, development, and use of smart city infrastructures adhere to the UN's Guiding Principles on Business and Human Rights. Risk assessment reports and associated procedures to mitigate risks must be carried out, published, and communicated effectively.

We consider the findings from this report as a first step towards equipping civil society and investigative journalists with the information necessary to push back against mass surveillance and repressive uses of technology in Myanmar and beyond.

"Public procurement is meant to provide for citizens' needs so it must be accountable to the public. Access to information is key to this accountability. Transparency of public procurement allows civil society to act as an effective watchdog on government systems, making recommendations for improvement and bringing this crucial area – where public and private sectors meet – under better public scrutiny."



Introduction

'Smart cities' is a term used by governments and companies alike to describe the use of digital technologies to facilitate and purportedly enhance public service delivery.[1] Initially coined as a marketing term by IBM in 2009 under its 'smarter cities' vision to enable cities to 'lead the way into a prosperous and sustainable future', smart cities are now also a policy objective in countries across the world.[2]

In 2018, the Association of Southeast Asian Nations (ASEAN) member states launched the ASEAN Smart Cities Network (ASCN) to encourage the integration of digital services in 26 cities towards the overarching goal of smart and sustainable urban development.[3] As is typical in smart city narratives, the ASCN views technology as an **enabler** of progress and innovation that will eventually benefit individuals living in smart cities – the assumption is that greater data collection and installation of sensors will facilitate the seamless delivery of services and resource management across the realms of transport, sanitation, healthcare, governance, and more.

While the promise of smart cities seems almost utopian on paper, several human rights challenges emerge from their design, development, and deployment. Various organisations, including ARTICLE 19, have warned against the uncritical adoption of emerging technology for solving complex social problems.[4] IBM's initial foray into smart cities included controversial projects in Davao city that may have facilitated horrific human rights violations.[5] A 2019 study in Pune, a well-regarded smart city in India, has shown that while sanitation projects focusing on 'smart toilets' and 'smart health' may consider the needs of those who use the toilets, they fail to consider the impact on those who **clean** the toilets. Sanitation work is deeply stigmatised in India and typically forced onto people from lower castes, specifically Dalit women. The study has shown that smart projects do not consult these women at all during any phase of their design or development. As a result, such projects are exclusive from the outset, raising key questions around the extent to which these women may be surveilled during their work without their consent. Furthermore, the privatisation of such public functions dilute government accountability to sanitation workers more broadly, raising further questions around how these businesses could be held accountable

should they fail to provide decent wages, proper working conditions, and job security for those who clean the toilets. In other words, are these projects truly 'smart' if they continue to perpetuate decades of oppressive practices?[6]

Overarchingly, smart cities are built on the idea of greater data collection (including biometric data) and sharing, with significant implications for the exercise of human rights, including the right to freedom of expression, the right to protest, the right to peaceful assembly, and the right to privacy. Smart cities also impact economic and social rights, particularly as 'smart' infrastructures now act as gatekeepers to critical sectors in everyday life, from immigration to availing government benefits and from healthcare to employment.

The design, development, and deployment of smart cities involve complex systems of decision-making that is often done behind closed doors, with little to no involvement from the public or civil society. Smart cities are usually the product of public–private partnerships between city or national governments and companies that provide the infrastructure and 'smart' technology including cameras, monitors, algorithms, sensors, and so on.[7] The vision for smart cities is promoted not just by the companies selling products alone, but also by management consulting giants aiming to paint a picture of more liveable, efficient cities in the future.[8] Within the umbrella of smart cities, technology procurement can reveal a lot about how state actors organise their priorities around governance and public service delivery. Peering into the process of procurement also reveals how and why certain technologies make it to the stage of deployment and point to accountability mechanisms (or lack of) within this process.

Overarchingly, smart cities are built on the idea of greater data collection (including biometric data) and sharing, with significant implications for the rights to freedom of expression, the right to protest, the right to peaceful assembly, and the right to privacy.

Smart cities also impact economic and social rights because 'smart' infrastructures now act as gatekeepers to critical sectors like immigration, healthcare, and employment.

In this report, ARTICLE 19 and Digital Rights Collective investigate how one particular component of smart cities in Myanmar – CCTVs – are procured.

This is an important area of investigation for several reasons.

First, CCTV cameras form the infrastructural backbone of a host of emerging technologies – including AI applications like facial and emotion recognition. The mission creep embedded in technical and policy design for CCTVs go from simply being installed cameras for 'safety', to being equipped to carry out remote biometric identification. Verification capabilities are normalised across policy documents but are rarely logistically understood. We focus on CCTV infrastructure generally, not just on one specific application like facial recognition or automated number plate recognition, as it is often technologies like traditional CCTVs which facilitate the easy transition to AI-based surveillance simply by layering on newer applications without adequate scrutiny. In this report, we trace how CCTVs as an infrastructural building block of smart cities, in particular, are installed in the first place and ask how they may evolve in the future. We analyse these developments through a human rights lens. We also provide a preliminary analysis of CCTV installation in three cities in Myanmar to help the reader understand these developments against the background of national priorities.

Second, this research is published at a particularly unique juncture in Myanmar's political reality: it began when the civilian-elected National League for Democracy (NLD) government was in power, and subsequently developed during and after the military coup in February 2021. There was an intensifying crackdown against protesters and activists in Myanmar after the military coup. As the new State Administrative Council formed after the coup, taking control of the country's legislations, governance, infrastructure, and technology, concerns surrounding potential uses and impacts of smart cities' infrastructure have evolved and become increasingly urgent. Images of authorities monitoring protest movements in traffic control centres were shared over social media.[9] With the military authoring new legislations and taking control of infrastructure and technology, there are increasing indications that the existing smart cities' infrastructure will be used to monitor people who are engaged in civic participation and exercising their rights to free expression.[10]

Third, CCTV technology and the various face, emotion, gait, and number plate recognition capabilities it can facilitate have enormous implications for human rights. The indiscriminate growth of CCTV networks facilitates mass surveillance, with major implications for the right to privacy which in turn creates chilling effects on the freedom of expression and association. Selective adoption of CCTVs also exists, thus endangering the right to equality and non-discrimination. Cameras are installed in 'high crime' or crowded areas, which globally have been shown to have a disproportionate focus on historically disadvantaged groups along the axes of class and socioeconomic status, among others.[11] It is important to remember in the context of Myanmar's current political climate that footage from traditional CCTV cameras can be used to conduct retrospective biometric identification and analysis, whereas newer CCTV cameras tend to come equipped with these capabilities.

Methodology and theoretical basis

Our initial research methodology to understand Myanmar's smart city involved conducting a scoping exercise based on interviews and desk research to understand the nature of smart city projects, and then subsequently planning to approach the implementing members of the Mandalay smart city committee or Mandalay City Development Committee (MCDC) to gather any information they would be willing to share for analysis. We chose Mandalay as a vantage point to understand smart cities and AI in Myanmar as Mandalay has been garnering recognition for its efforts in implementing smart cities,[12] while the MCDC also had higher civic engagement. We planned to combine the data they shared with the information from government tenders and announcements of the smart city projects. After that, before the research concluded, we hoped to conduct consultations with Myanmar civil society to include their concerns.

However, it was not possible to pursue this method after the military coup, due to the risks involved for researchers working under the drastically changed political landscape, and also because members of the MCDC have been in hiding or are being detained by the military junta. Therefore, we realigned our plans to gather as much available information as we could from media reports, investigative journalism, and leaked documents and tenders from the government to map out the extent to which surveillance systems and AI technology infrastructure had been developed in Myanmar's cities, especially within the new context of the military dictatorship.

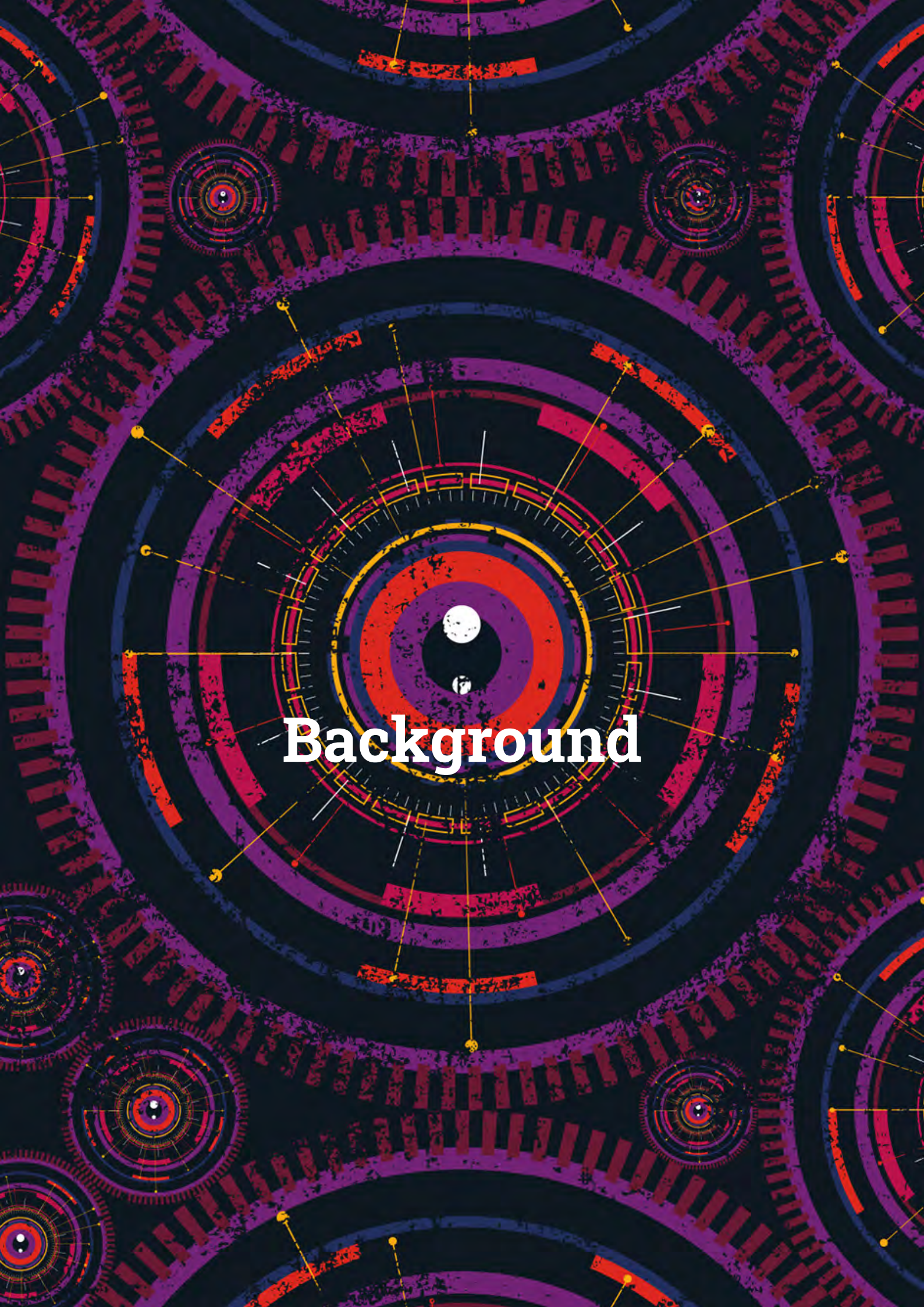
Our understanding and analysis from the scarce information that is available online and from interviews misses the rich detail we could have uncovered through field engagement. Yet our analysis of the government, media, and civil society narratives offers the first step to foreground the gravity of the dangers of the state surveillance used by the regime on civilians in the near future. Our second difficulty is the inability to verify some of the information collected from reports. Several pieces of information for different projects are still missing or not yet reported, and it remains risky to physically visit the project areas due to the pandemic and an unsafe political environment. Thus, we present the information we have as of now, as well as the information we do not have, as one of the findings to highlight future areas of investigation.

Before the military coup happened, we managed to conduct interviews during the initial scoping phase with individuals from eight civil society organisations working mainly on digital rights and technology, and those working with the government. We originally planned to use these findings to formulate questions and topics to interview people directly involved in implementing the smart city in Mandalay. As we resumed this research after a hiatus from research activities during the early months of the protests, our researchers, who are members of Myanmar civil society, obtained leaked government documents and tenders from close contacts. We searched across a total of 1,932 tender documents from 2020 using the following keywords – 'cameras/ကင်မရာ', 'CCTV', 'control room', 'machine/စက်', 'Monitor', 'Tech/နည်းပညာ', 'AI', 'safe city', and 'smart city'. We extracted a total of 11 surveillance-related tenders in both Myanmar

and English language announcements. In addition, we collected other government announcements and news reports and investigated pieces that came out after the coup.

Our mapping focuses on stages of procurement as we find that a number of systemic issues are rooted in how and why technologies are purchased in the first place. Although local media reports have given much attention to the billion kyats (as per the 2019 exchange rate this would be approximately USD 675,000, as per the 2020 exchange rate this would be approximately USD 540,159) spent on CCTV megaprojects with Huawei, the focus has primarily and exclusively been on Chinese involvement and potential spying[13] through backdoors, as opposed to a systemic analysis of public procurement. These findings are important but run the risk of missing crucial insights into the procurement process that state actors in Myanmar are pursuing to buy this technology, regardless of where it is coming from.[14]

Our focus on CCTVs – as opposed to a specific type of AI technology like facial recognition – is a deliberate one, as we view CCTVs as an entry point to understanding the larger ecosystem of smart cities in Myanmar. CCTVs do not exist in isolation within smart cities, but rather, as discussed earlier, form an integral prerequisite for many smart city infrastructures to exist and function. This approach enables us to analyse broader goals implicit within Myanmar's 'smart' future – a majority of government documents simply refer to CCTV cameras at the time of procurement, without specifying what kinds of surveillance capabilities they wish to implement, such as face recognition, emotion recognition, gait recognition, automated number plate recognition and so on. We highlight this elision throughout the document.

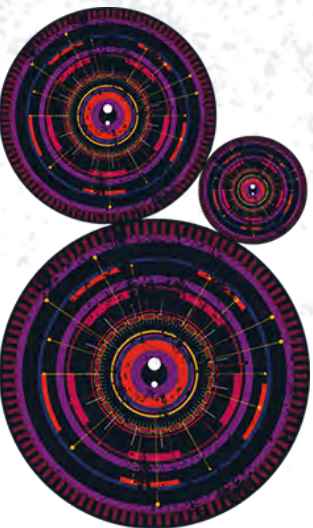


Background

On smart cities, safe cities, and political realities

After coming out of a five-decade-long military dictatorship in 2010, the Myanmar military (Tatmadaw) relinquished their power to transitional civilian governments for a little over 10 years, during which time the country made notable progress as a democracy. In 2015, the long-time opposition party against the military, NLD won a landslide victory in the second general election since the transition, under the leadership of Myanmar's icon of democratic struggle, Aung San Suu Kyi, and became the first government with popular civilian support. However, this reign of power was not without grave problems either – during the military operation that forced out more than 730,000 Rohingya, the NLD government stayed silent, and Aung San Su Kyi rejected the accusations of genocide against the Rohingya in The Hague.[15]

Between 2010 and 2021, a focus on technological development as a marker of democratic progress became gradually apparent. Smart city achievements were lauded as progressive developments in a country coming out of decades of dictatorship and are at the centre of a rapidly growing surveillance infrastructure in Myanmar.[16] Of all the cities across Myanmar, Mandalay has received much media attention compared to other cities for the openness and progress of the MCDC, the administrative body of Mandalay. Members of MCDC have been relatively more engaging than other regional governments, evidenced by the availability of information in media, reports,[17] and the committee's appearances in public interviews. The Mandalay government promoted and touted AI-driven smart cities as the enabler of success and modernisation during the five-year NLD terms.[18] This is galvanised by regional recognition for their progress in implementing technology-enhanced public services; the implementation committee received an award[19] and Mandalay was ranked fifth[20] in Southeast Asia's top 10 cities in the process of becoming a smart city in 2018. Just a few months before the end of the NLD term



and before the coup in 2021, the Mayor of Mandalay, Dr Ye Lwin,[21] posted on his Facebook profile a list of city development projects achieved during his term, many of which were smart public services. On the other hand, both Yangon (the largest commercial city in Myanmar) and Naypyidaw (the administrative capital and seat of the government) were also part of Myanmar's pledge to the ASCN. However, both cities focused on other projects like public housing in their smart city action plan,[22] while Mandalay's focus was heavily on other public services.

Driven by ASEAN recognition and an award, the MCDC has strived to push the integration of AI into its infrastructure as part of its 30-year plan.[23] Services include GPS to track garbage disposals, remote sensors to control traffic flows, smart technology for solid waste management, smart payment for Mandalay's digital payment system, and CCTV installation in crime-heavy neighbourhoods, to name a few. By 2019, MCDC had a fully operative control centre[24] where the officers monitor traffic flows and congestion on 13 screens and adjust the sequencing of traffic lights accordingly through the detection of the sensors installed in CCTV cameras.

At the same time, other cities were also integrating AI into public spaces, albeit not under the smart city umbrella. For example, since 2018, Yangon has been setting up smart payment for buses, while installing CCTVs across the city in traffic lights, popular public areas, and airports that are not necessarily under the frame of 'smart city' projects in media or government narratives. According to interviews conducted for this project, a member of the Yangon IT development committee informed us that the committee had been less transparent about such projects compared to Mandalay. Under the NLD government, one of the primary reasons given for the CCTV installation was to 'empower police by complementing the lack of police staffing in preventing crimes to make places safe'.[25] The Myanmar Government has been well versed in using this justification of safety to exert control; one of the most notorious examples is the 'guest registration' law, whereby a visitor staying overnight at a person's house needs to register at the neighbourhood administrator appointed by the government. This law was practised throughout the old military regime and removed during the NLD

government due to public criticism. The new junta re-enacted it amidst the growing protests in February, along with other legal amendments that corrode individual freedom.

CCTV installation in Myanmar's smart cities is part of a longer legacy of surveillance in Myanmar and sits at the juncture of two overlapping policy initiatives. The first is that of 'smart city' initiatives which, as discussed earlier, were conceived as part of NLD's different regional governments to digitally equip Myanmar's large cities – Yangon, Mandalay, Naypyidaw, Monywa, and Mawlamyine – with AI technology.[26] The second is that of 'safe city' plans that focus on CCTV installation in specific civic spaces like residential neighbourhoods in Mandalay and Yangon, as well as citywide CCTV installation in Naypyidaw.[27] These include AI and data-based projects, CCTV installation with facial recognition, and vehicle licence plate recognition. Surveillance cameras and CCTV infrastructure form an integral part of both initiatives given their long legacy in Myanmar's surveillance practices. The companies supplying this technology include Chinese giants like Huawei and also local companies as discussed later in the report.

The Myanmar Police Force has also long relied on tracking vehicle licence plate numbers to track down people. Car ownership in Myanmar is a tightly controlled system with elaborate registrations using the owner's personal information such as name, identification number, and address. There are no data protection or personal privacy protection laws that allow or limit how much the police or 'authority' can access the data of a car owner. The government has projected a narrative of vehicle tracking as an effective crime-fighting method since previous junta times. Current CCTVs with number plate recognition can alert the police if an unwanted or suspected car comes into sight.

On 1 February 2021, the military rule returned just a few months after the third general election, when the Tatmadaw led by its current head, Senior General Min Aung Hlaing, staged a coup d'état, detaining the leader of the NLD party and the President along with other NLD government officials, activists, and the artists, and thus ending a short-lived democratic period in the country.

Protests against the military coup have taken place on streets across almost all cities in Myanmar since February 2021, often occurring organically and spontaneously in many municipalities and large cities. Since the beginning of the coup, thousands of people have organised peaceful civil disobedience movements, boycotts, and protests in the early days, and armed struggles at the later stage, to resist the coup and demand the return of democratic rule and the release of the people detained. Over a year after the coup, peaceful protests are being cracked down on brutally and inhumanely by security and police forces deployed by Tatmadaw. The Assistance Association for Political Prisoners (Burma) reported as of 1 October 2021 that there were 1,146 people killed, 8,584 arrested, and 6,921 detained in relation to the military coup since 1 February 2021.[28] The military's Ministry of Transport and Communications announced it would include codes of regions and townships of a vehicle's licence plate as a 'security feature' starting by the end of July 2021.[29]

"CCTV installation in Myanmar's smart cities is part of a longer legacy of surveillance. Since February 2021 the military has turned these cameras into a weapon – to track and arrest those who dissent."

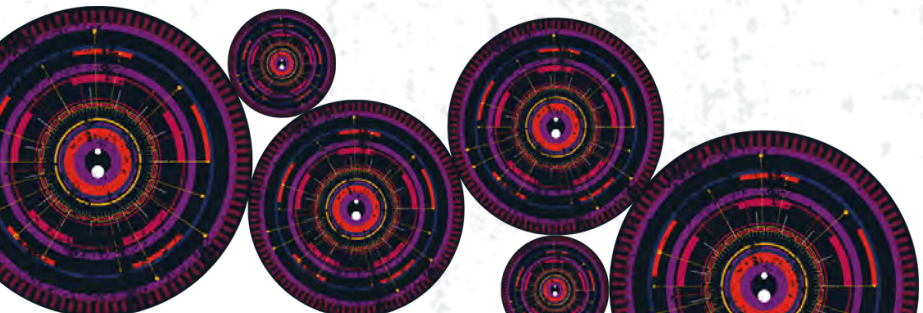
After the military took power in February 2021, the Tatmadaw took command of the CCTV control centres across Myanmar, making CCTVs a new kind of weapon when repressive forces seize central authorities. Concerns around the chilling effect of CCTVs on freedom of expression arose almost immediately – people protesting against the coup raised concerns that the military was using these systems 'like a digital dictatorship – the regime is using technology to track and arrest citizens, and that's dangerous'.[30]

Responding to concerns about the increasing use of surveillance technology, Huawei has maintained that they merely provide 'standard ICT infrastructure equipment'.[31]

But infrastructure is not as innocuous and non-controversial as Huawei makes it sound. During this intensifying crackdown against protesters and activists, images of authorities monitoring protest movements in traffic control centres were shared on social media.[32] With the military authoring new legislations and taking control of infrastructure and technology, there are increasing concerns that the Myanmar military can potentially utilise existing smart cities' infrastructure – such as Naypyidaw's fully functioning surveillance networks, Yangon's vast CCTV spread, and Mandalay's CCTV network – to monitor people who engage in civic participation and exercise their rights to civil liberty.[33]

In Mandalay specifically, after the coup disrupted the plans in 2021, the military ousted the incumbent MCDC by arresting[34] the Mandalay City Mayor, Dr Ye Lwin, who led the Smart City Project, and replacing[35] them with its own Mandalay regional council. The implementation of CCTV and other equipment, together with Huawei as part of the Mandalay Safe City, has reportedly transferred to the military in May 2021. The equipment arrived in February 2021.[36] It is not yet clear at the time of the writing how the implementation will unfold under the military council's management. Two local companies, ACE and Zarni Electronics, won tenders to install the equipment, but information or specifications about such tenders could not be found. CCTVs equipped with face and licence plate recognition are connected to servers accessible by police stations. The seeds for Mandalay's surveillance system pre-date the coup – and despite this new deal with Huawei to ramp up 'security', Mandalay already had over one hundred monitors[37] that were monitored by the police command centre since 2015.[38]

One of the major concerns expressed by civil society representatives interviewed for this report was the restriction on the freedom of movement and civic participation that smart cities more broadly could impose. Civil society activists stated that CCTV networks with facial recognition systems are on the horizon and that they could be used



to identify and monitor activists who have been most vocal about the government, effectively restricting their freedom of movement and freedom of assembly. Under the NLD government, special police (the police from the Special Branch of the Special Intelligence Department) used camera footage against activists in legal cases.[39] Since the coup, protesters have expressed fear that footage from the CCTV cameras linked to public networks and private residences has been used by the military to track or arrest them.[40] As civil society expressed in interviews, they fear surveillance technology would increase the NLD government's control on freedom of assembly, thus shrinking civil society space. This has now become a reality when the military is empowered by the same surveillance technology.

Thousands participate in a protest organised by the General Strike Committee of Nationalities to denounce the military coup and call for federal democracy in Yangon, Myanmar.
Photo: February 2021, Digital Rights Collective.

"CCTVs are typically justified by claims that they will monitor, detect, and prevent theft and fraud, and maintain public order. They create the impression of being watched, either by powerful entities who could be the owner of a private establishment, security personnel, or more commonly, the state. While this narrative has inspired heavy investment into the installation of CCTV systems, the enthusiasm around CCTVs is rooted more in their perceived potential than actual impact."

On CCTVs

Significant global adoption of CCTV cameras has followed since they came into existence in 1942. The technology has transitioned from being used in military contexts to being adopted in various aspects of daily life, most prominently to facilitate policing activities. In 2004, academic experts[41] explained its expansion in public spaces through four stages:

1

The first stage is the adoption of CCTVs through the private sector to monitor banks, shopping malls, and commercial establishments to prevent theft and fraud.

2

Stage two marked the use of CCTV in the 'key institutional areas of the public infrastructure' such as schools, town halls, public libraries, and the transport sector. This particularly occurred in the mid-1990s either because laws relating to public space surveillance were relaxed in some countries like France, or simply because CCTVs were slowly normalised through their use in the private sector.

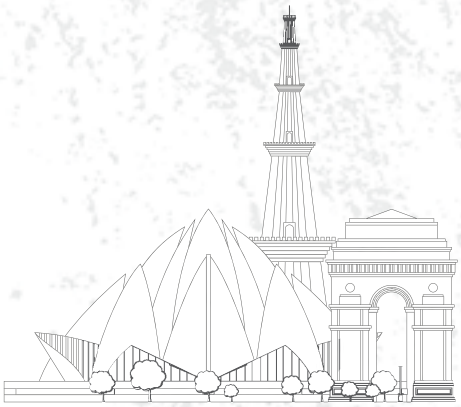
3

Stage three was run by public authorities under the guise of crime detection and prevention and involved the use of CCTV in public spaces such as town centres and streets.

4

Stage four indicates the adoption of CCTVs moving towards ubiquity, with 'hundreds of cameras providing blanket coverage of whole areas of a city'.

Nearly two decades after this classification by Norris et al., we are firmly at stage four. Currently, India's capital **New Delhi** holds the record for having the most CCTV cameras in the world, with 1,826.6 cameras per square mile, followed by **London** (1,138.5 cameras per square mile), **Chennai** (609.9 cameras per square mile), and **Shenzen** (520 cameras per square mile).[42]



NEW DELHI

1,826.6

cameras per square mile

LONDON

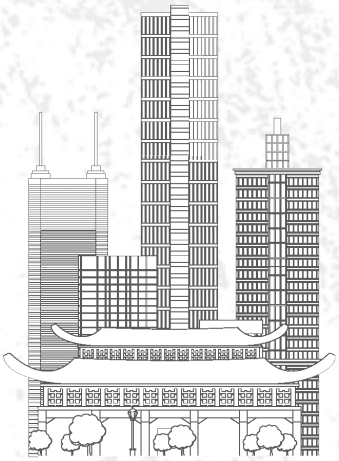
1,138.5

cameras per square mile

CHENNAI

609.9

cameras per square mile



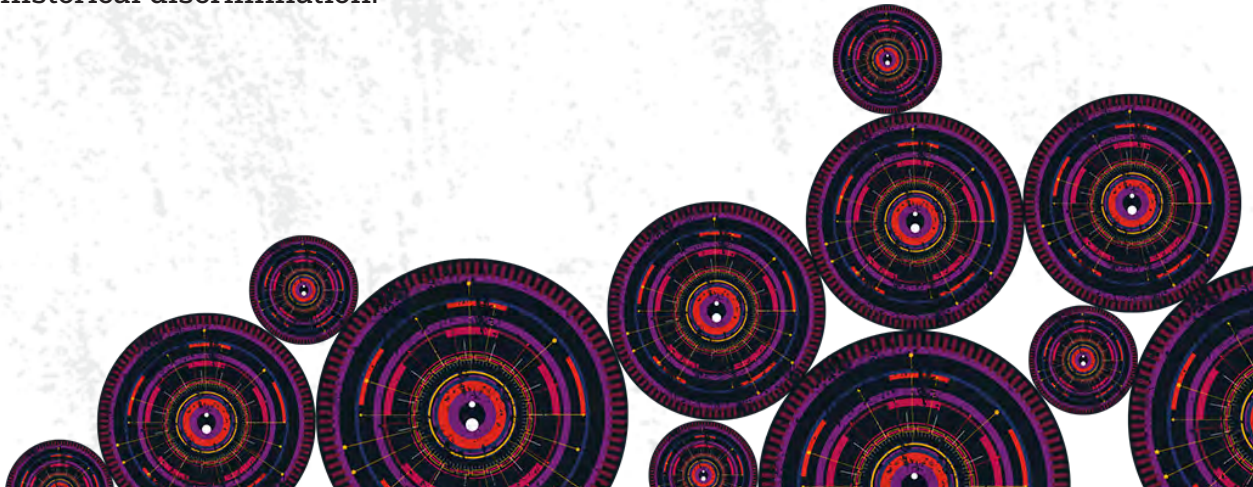
SHENZEN

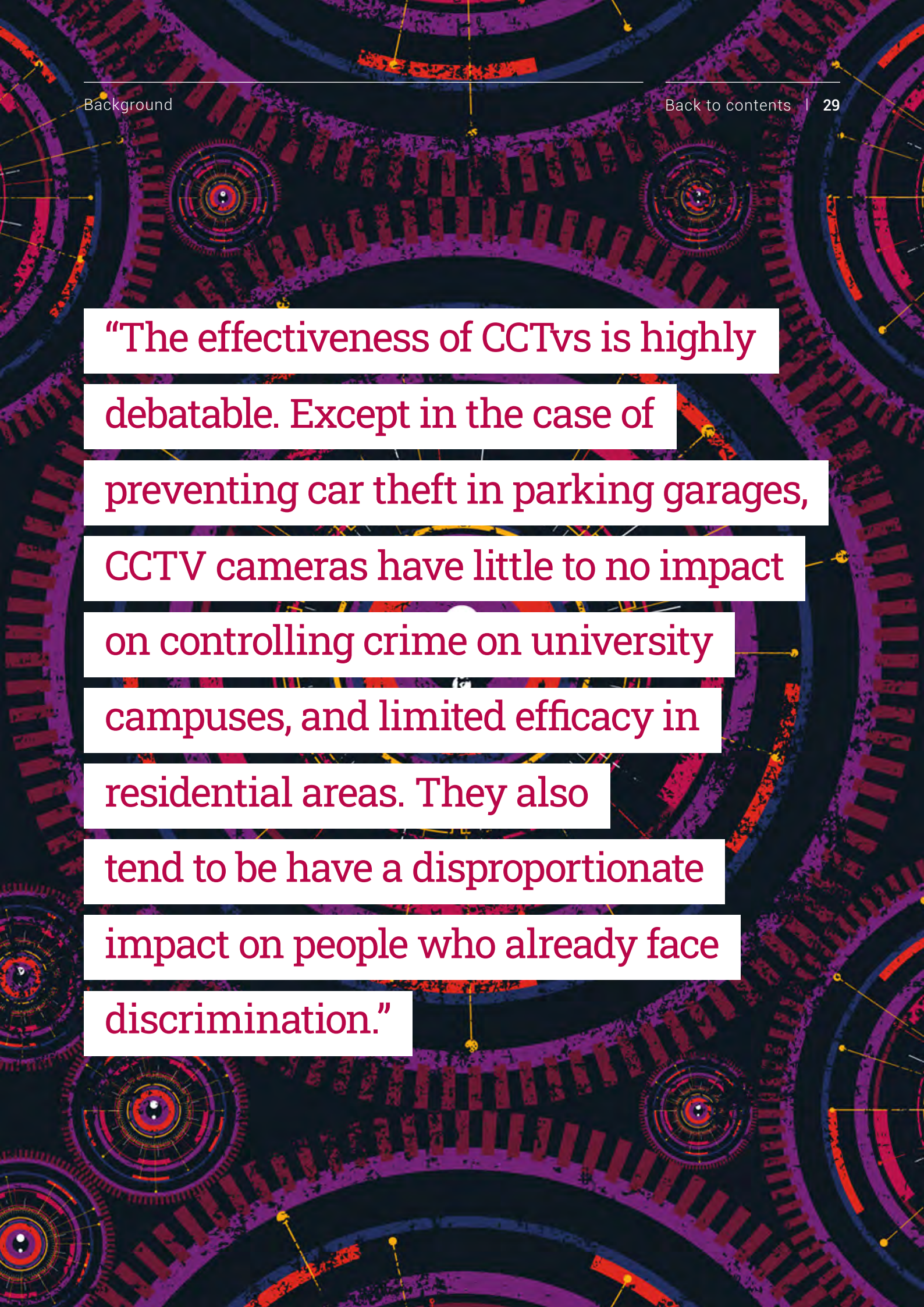
520

cameras per square mile

The justification offered for the deployment and use of CCTV networks has consistently been to monitor spaces, prevent and detect crime, particularly theft and fraud, and maintain public order. The installation of CCTVs provides individuals with the impression of being watched, either by powerful entities who could be the owner of a private establishment, security personnel, or, as is increasingly common, the state. While this narrative has inspired heavy investments into the installation of CCTV systems across the board, the enthusiasm around CCTVs is rooted more in their perceived potential than actual impact.

The effectiveness of CCTVs is debatable – Norris et al. suggest that 'It would appear that the global rush to install CCTV in public spaces has also been carried out with little systematic attention to the issue of evaluation. But it is the symbolic value of CCTV that is perhaps most important.'[43] It is also telling that the illusion of safety is a crucial component of CCTV adoption – Norris et al.'s research found 'In different countries, at various moments, crises, triggered by particular events such as a child-kidnapping, a class-room murder, a terrorist outrage or rising concerns over crime, will lead to calls for the extension of video surveillance.' Their findings are consistent with trends observed over the years across multiple jurisdictions. The rush towards increased video surveillance after the 9/11 attacks is testament to this fact, and also applies beyond the USA: prior to 9/11, and after terrorist bombs were planted in London's financial district in 1993 and 1994, the UK Government installed a 'ring of steel' – a network of CCTV cameras – in response.[44] This is puzzling given that research on CCTVs has found that except in the case of preventing car theft in parking garages, its use has not been found to reduce violent crime.[45] Further, CCTV cameras have little to no impact on controlling crime on university campuses,[46] limited efficacy in residential areas,[47] and has a disproportionate impact on surveilling communities that have faced historical discrimination.[48]



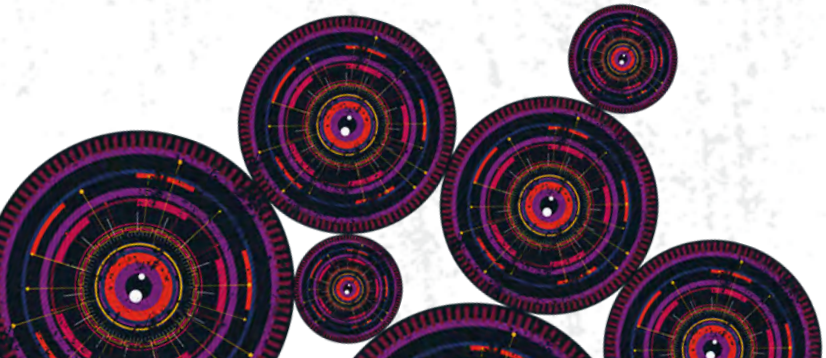


"The effectiveness of CCTvs is highly debatable. Except in the case of preventing car theft in parking garages, CCTV cameras have little to no impact on controlling crime on university campuses, and limited efficacy in residential areas. They also tend to be have a disproportionate impact on people who already face discrimination."

As CCTVs are cemented into the fabric of public and private spaces, it paves the way for the normalisation of mass surveillance. CCTV systems not only symbolise watching people in real time, but the ability of these networks to store information also means that people's actions, behaviours, interactions, and expressions are subject to scrutiny and analysis both in real time and in retrospect. With the additional layer of biometric surveillance, CCTVs now don't just watch what is happening, but rather track **who** is doing **what** and, in the case of emotion recognition, are also used to determine **what type of person** an individual is. In the context of CCTVs in public spaces, the existence of public–private partnerships that bring these systems to deployment is also important to consider, particularly given their implications for the freedom of expression, right to privacy, and the right to peaceful assembly and association. Procurement processes that lay down specifications for monitors, cameras, training personnel, etc, are often negotiated behind closed doors to the extent that the installation and use of CCTVs only become public knowledge once it is already in place, as opposed to being subject to rigorous public debate and scrutiny before adoption.

CCTV evolution and integration with AI

CCTV networks today readily plug into wider technical networks like smart cities and are easily equipped with AI-based applications like face and emotion recognition. The technical infrastructure of cameras and stored video feeds serve as the first step for these newer forms of surveillance infrastructure to function.



Myanmar's legal framework

Myanmar has a common law system created under the British colonial government in the 1950s. Before the 'civilian' government, led by ex-general Thein Sein, there was a denial of basic human rights, arbitrary arrests, and abuses. After the 8888 Uprising in 1988, the military ruled by decree for over two decades.

Myanmar's 2008 Constitution was drafted as part of the 'Seven Step Roadmap to Democracy'.[49] The Constitution recognises the right to freedom of expression and freedom of assembly, and limited aspects of privacy; however, the reasonable restrictions provided fall short of international standards as these rights are only granted to the extent that they 'do not contradict laws for the protection of national security, public order, community peace and tranquillity, and public morality'.[50]

When the Thein Sein government came into power in 2011, censorship and surveillance reduced to some extent. Some laws which provided guarantees for freedom of expression were passed, such as the Telecommunications Law, Law Relating to the Right to Peaceful Assembly and Peaceful Procession, the News Media Law, and the Printing and Publishing Enterprise Law.[51] These amendments, however, did not stop the government from using other existing laws to arrest pro-democracy activists, journalists, and human rights defenders.

Civil society organisations pushed back on articles which violate or could violate human rights, such as Article 66 (d), of the 2013 Telecommunications Law which criminalised 'defamatory' speech.[52]

Further, the excessive secrecy that characterised the previous governments did not reduce, with the Official Secrets Act (1923) remaining unreformed and used aggressively against journalists. Efforts to adopt a right to information law started in 2016 but were limited.[53] There was a brief flirtation with joining the Open Government Partnership, a multilateral initiative that aims to secure concrete commitments from

national and sub-national governments to promote open government, empower citizens, fight corruption, and harness new technologies to strengthen governance. This idea was ultimately dropped. Thus, the mechanisms for the public, civil society organisations, and journalists to be able to obtain information about smart cities implementation, any protections, problems, abuses, or other issues, is virtually non-existent.

"In the context of smart cities, it is crucial to note that Myanmar currently does not have a data protection framework.There are no legal requirements for transparency of the operations of CCTV systems, and individuals cannot demand to know what information is held about them, or how it is being processed and used by the operators or third parties such as government bodies."

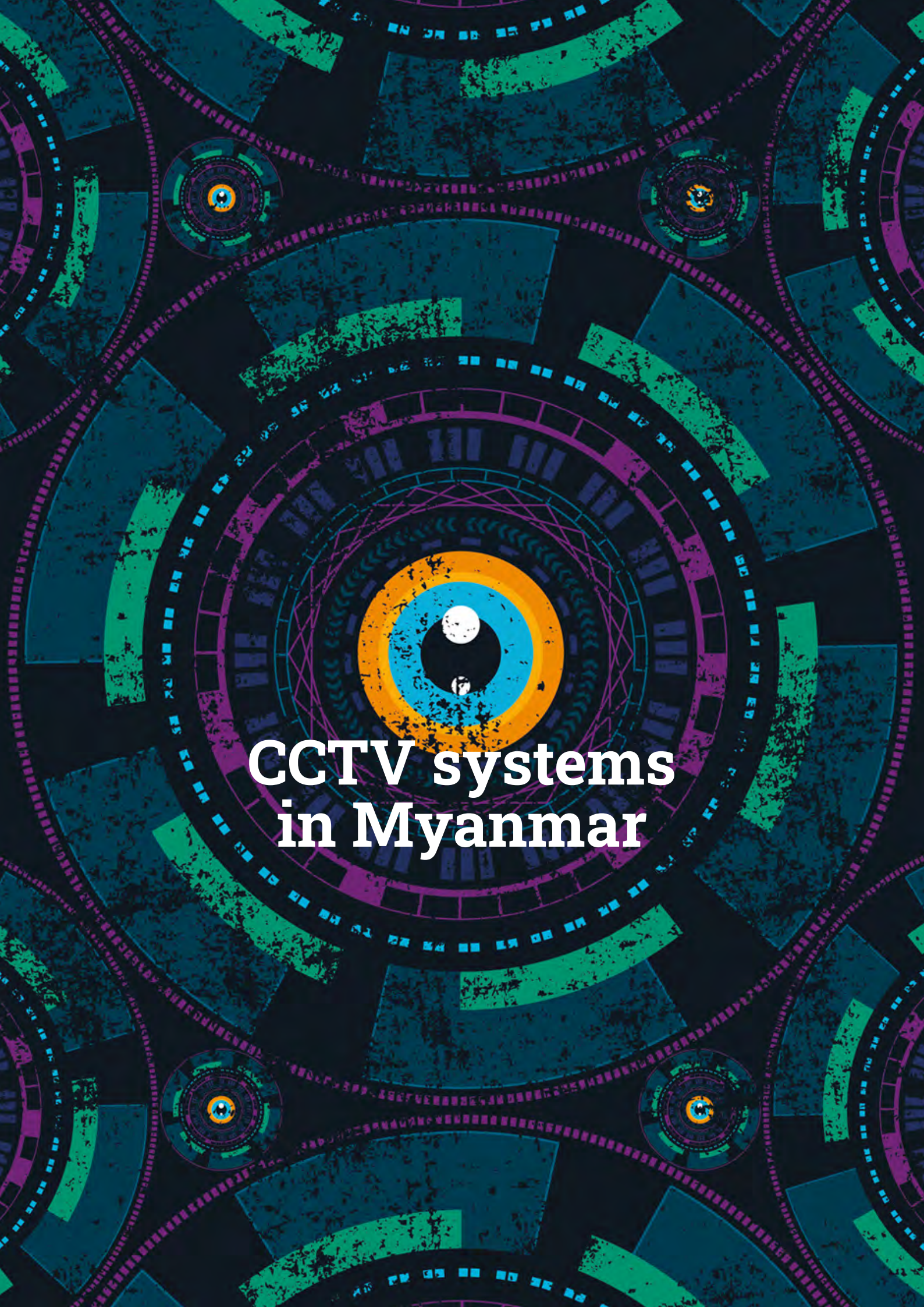
Interviewees explained that when it comes to smart cities and CCTV, under the 2017 Citizen's Privacy and Security Law, surveillance needs to be carried out with the approval of the 'relevant' ministry, in this case the Ministry of Home Affairs. Governments that want to install CCTV will thus need approval from the Parliament and/or the Ministry of Home Affairs. In the context of smart cities, it is also crucial to note that Myanmar currently does not have a data protection framework.[54] Further, this lack of data protection laws, which are in place in over 120 countries worldwide including China, Malaysia, and Thailand, limits the accountability and transparency of the use of the systems, as there are no legal requirements for transparency of the operations of the systems, nor the ability of individuals to demand what information is held about them, or how it is being processed and used by the operators or third parties such as government bodies.

Over the past few years, the cybersecurity and cybercrime law has been one of the priorities of the NLD government. According to the interviewees, in 2020, the NLD government was separating cybersecurity

and cybercrime into two distinct frameworks. The Ministry of Transport and Communications was planning to draft legislation only focusing on cybersecurity. The interviewees also stated that it seems the cybersecurity framework will be focusing on security rather than data protection and digital rights. The Myanmar Centre for Responsible Business has published its policy brief on cybersecurity and cybercrime framework highlighting the need to address cybercrime, actions to increase cybersecurity, and the steps for developing good cybercrime laws as well as to avoid violations when implementing the law.[55]

In Myanmar, the implementation of projects does not depend on relevant legislation being in place. For instance, the Ministry of Transport and Communications invested MMK 6,190 million (roughly USD 4 million) towards implementing a Lawful Interception System for the 2019–2020 financial year, even though Myanmar does not have a legislative framework for interception to this date.[56] In the context of smart cities, the implementers from Mandalay MCDC mentioned their concern for lack of data protection, but yet they still went ahead with putting in place 'smart' infrastructure because they were not the ones enacting legislation.

Since the coup began, the military junta has amended laws that protect human rights. The amendments enable arbitrary arrests, remove basic privacy protections, and criminalise peaceful protests. These developments, in tandem with an increasing reliance on repressive technology, indicate a systematic build towards the erosion of human rights. For example, under the Law Protecting the Privacy and Security of Citizens, sections 5 (pertaining to safeguards relating to search and seizure), 7 (requiring a court order for any detention of more than 24 hours), and 8 (protecting an individual's right to privacy) were suspended as of 13 February 2021. Other legislations amended include the Law Protecting the Privacy and Security of Citizens (2017), the Penal Code 505 (A), the Ward and Tract Administration Law, the Code of Criminal Procedure, and the Electronic Transactions Law.[57]



CCTV systems in Myanmar

The spread of CCTV systems across Myanmar

December 2015

At the Mandalay Police Command Centre, 80 CCTVs are set up with 130 monitors

May 2016

A CCTV traffic centre is launched in Yangon: a total of 140 intersections across 25 townships have been fitted with CCTV relays since February 2016 at a budgeted cost of MMK 2.5 billion

March 2019

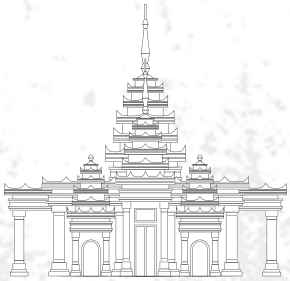
The tender for installation in Naypyidaw is announced and awarded to two companies founded by the former military general's family member: Naung Yoe for cameras and cables installation, and Linn IT Solution for the construction of a control centre

April 2019

The Chief of Police of the Myanmar Police Force visits China to meet with Huawei

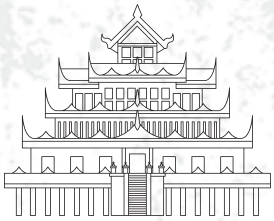
June 2019

The Yangon Regional Government announces that China has provided 240 surveillance cameras for Yangon, with a total of 2,995 CCTV cameras installed in 1,138 places across Yangon



August 2019

Mandalay Traffic Control Centre monitors traffic flows from 13 screens showing traffic congestion and adjusts the sequencing of traffic lights through the detection of the sensors installed in CCTV cameras

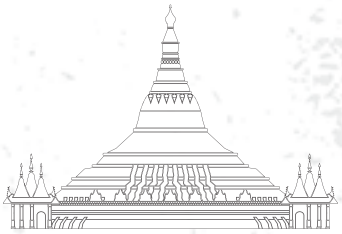


April 2020

Naypyidaw Development Committee installs 49 CCTVs and related components at the City Hall and at gates to housing compounds

May 2020

The government holds a Swiss challenge for the tenders and awards Huawei the contract in Mandalay



May 2020

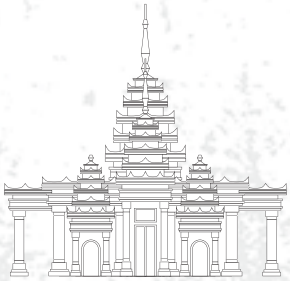
The Yangon Region Police Office has seven locations and three control rooms to monitor the Yangon–Mandalay Highway in Hlegu

June 2020

Yangon Maritime Police and the Ministry of Home Affairs call for open tenders for 120 CCTVs and two monitoring control rooms with 16 LCDs for eight ports and nine bridges along the Yangon River

July 2020

MCDC calls for open tenders to install individual loop sensors at traffic points in six townships



July 2020

MCDC and the Building and Central Store Department launch a tender for the installation in six townships of an individual loop censor traffic point, traffic lights with a computer system, and CCTV cameras

July 2020

Yangon Region Police Force with Yangon Regional Government launch a tender to install CCTV cameras in nine territories within the Yangon Region

November 2020

Huawei is awarded a MMK 1.9 billion contract for AI-powered CCTVs for Mandalay's Smart City project

December 2020

335 Huawei CCTV cameras with AI and face recognition go live in Naypyidaw, costing MMK 4 billion (USD 2.9 million)

December 2020

Yangon City Development Committee launches a tender to install CCTV cameras

Overview of existing systems

Mandalay

The 'Mandalay Safe City' project is one of the plans of the smart city initiative to reduce crimes in Mandalay: the city administration signed a MMK 1.9 billion (USD 1.02 million) contract with Huawei in November 2020[58] to buy AI-powered CCTVs with facial recognition capabilities.[59] The second biggest city and central economic seat of Myanmar, Mandalay is also known as the royal capital of Myanmar. It has been depicted as a beacon of progress with the development of its smart city infrastructure and has also received international accolades for developments within the city.[60] As part of a broader master plan, the MCDC took the lead in implementing digital technology integration in their public services.[61]

The project planned to install CCTVs in three out of seven neighbourhoods in Mandalay – Mahar Aung Myay, Chan Mya Thar Si, and Pyi Gyi Tagon – within 6 months. These neighbourhoods were chosen due to a higher crime tendency, reportedly claimed in the survey carried out by district police and Huawei.[62] This is not particularly unique to Myanmar – researchers have found that surveillance exports from China tend to be adopted in countries with high crime rates, even if the adoption has no eventual impact on reducing crime levels.[63] Cameras will be linked to the MCDC control centre.[64] Based on conversations with Mandalay locals, the selection of these neighbourhoods is questionable given that these neighbourhoods had lower incomes but did not seem to have a higher crime rate relative to other neighbourhoods in Mandalay. Further to this, the crime indicators that led to the survey outcomes, as well as the survey itself, were not published.

The roots of these developments extend back by at least four years. In 2018 and 2019, officials from the Mandalay Police Force and the Myanmar Chief of Police visited[65] Huawei offices in China. Huawei offered to support and provide the required technology for transforming Mandalay into a smart

city. As discussed in the following pages, the contract to buy equipment was given to Huawei without a due tender process, which led the Ministry of Transport and Communication to object to the decision and the project draft. Due to criticisms and concerns about Huawei's involvement[66] in possible spying, the Mandalay Regional Government 'carefully'[67] revised the contract draft in June 2019 and submitted it to the President's Office for review. There was a delay until May 2020, when the government held a Swiss challenge for the tenders and Huawei was again awarded the contract. A Swiss challenge is a procurement process that requires a public authority (usually an agency of government) which has received an unsolicited bid for a public project (such as a port, road, or railway), or for services to be provided to the government, to publish the bid and invite third parties to match or better it.[68] In July 2020, MCDC called for open tenders to install individual loop sensors at traffic points in six townships, according to the government's tender website.

Naypyidaw

In Naypyidaw, Huawei-made CCTVs had already gone live by December 2020. Under a Naypyidaw Council (a regional government body) project worth MMK 4 billion (USD 2.7 million),[69] 335 cameras with facial recognition technology and licence plate recognition were installed across eight townships in Naypyidaw.[70] The tender for installation was called in 2019 and awarded to two companies founded by a family member of the former military general: Naung Yoe Technologies for cameras and cables installation, and Linn IT Solution for control centre construction.[71]

The tender process did not indicate where CCTVs would be installed but it appears most major roads, traffic junctions, and toll gates are under surveillance – and possibly many more places that are not reported. According to the announcement from the companies and tenders, CCTVs have also been installed in Naypyidaw City Hall, housing compounds, the airport, and parliament buildings. Police have direct access to operate the Naypyidaw control centre, and will keep the footage for 60 days.[72] Given the lack of transparency about the process and specifications, it is not clear how Huawei's current role and status have come to exist.

Yangon

Yangon already has cameras installed at 154 traffic junctions, as well as surveillance cameras around popular areas such as City Hall, Inya Lake, and ShweDagon Pagoda. Current information in the public domain does not identify whether these cameras are AI-enabled. The traffic control cameras project started in 2016 and cost MMK 2.5 billion (USD 1.3 million).[73] The traffic control centre, based inside People's Park, opened in May 2017. Police have access to cameras installed on traffic lights, and these cameras, along with other technology in the control centre, are largely Chinese.[74] According to another media report quoting the Yangon Regional Government, the city has almost 3,000 cameras in over 1,000 locations.[75] In June 2019, the NLD's Yangon government publicly announced their plan to add 140 more surveillance CCTVs in Yangon's most crowded township, Hlaing Thar Yar, where most internal migrants working in factories live. Since then, not much has been reported on Hlaing Thar Yar's project or who was given the contract. In June 2020, Yangon Maritime Police called for open tenders for CCTVs and two monitoring control rooms for eight ports and nine bridges along the Yangon River. In July 2020, the Yangon Police Special Intelligence department also called for tenders to install CCTVs in nine territories within Yangon.

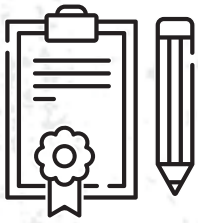
In May 2020, Yangon Regional Government allowed Yangon Police Force to call open tenders for a project to install a control centre as well as CCTVs in seven locations across 26 miles on the Yangon–Mandalay Highway from the Hlegu Township in Yangon City up to the border between the Yangon Region and Bago Region. According to an investigative article, these projects were underway before the coup and the implementer had special access from the police chief to work on and finish the projects even during curfew hours after the coup.[76] In December 2020, the Hmawbi City Development (Sipin/စည်ပင်) called for tenders for CCTV installations for the Hmawbi Township in the Yangon Region. The local police in Hmawbi also have a control centre for CCTV.[77] Tenders were granted to a company called FISCA which had close ties to the military and who had placed the cameras around ShweDagon Pagoda. FISCA sourced the equipment mainly from Huawei and Dahua.[78] FISCA is a Singaporean company that has worked with previous military juntas. The FISCA branch in Myanmar was founded in 1997 by a Myanmar national.

Public procurement process

Myanmar's legal framework for the public procurement process was established in 2011 as part of the country's political reforms and transfer to a civilian government. The procurement process itself was seen as an important marker of government integrity. An analysis of the government's Directive No. 1/2017[79] broke down the procurement process in Myanmar into three stages: pre-tender, tender, and post-tender.[80]

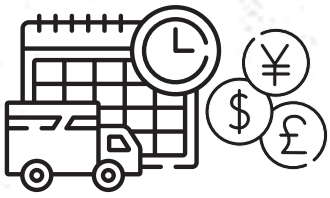
1

Pre-tender consists of the preparation of an annual budget and budget allocation to government agencies, procurement planning to identify procurement needs and procurement approach, defining procurement requirements, and preparing tender documents.



2

The **tender stage** is an invitation for potential suppliers to submit tender proposals, evaluate tender proposals, select the winning tender, and award the contract.



3

The **post-tender stage** is the contract management to ensure the supplier delivers goods or services of required quality and is paid as per the terms of the contract.[81]

According to Directive No. 1/2017, tender procedures are to be followed by the government departments and organisations in construction, purchase, procurement of services, lease, and sale. Article 10(a) states that a value of less than MMK 10 million (USD 5,400) does not require calling for a tender; however, the Tender Committee must request fee proposals from at least three trustworthy companies. Article 10(b) states for projects valued from MMK 10 million to MMK 100 million (USD 5,400–54,000), the tender announcement has to be published two weeks before the tender opening date on the notice boards of the relevant ministry, general administration department, and the district and township administration office. Article 10(c) states for projects over MMK 100 million (USD 54,000) the tender has to be announced at least twice in state-owned newspapers one month before the tender opening date, on relevant department's notice boards and, if possible, on the ministry's website.[82]

Despite the public procurement process outlined above, the Mandalay Regional Government directly awarded the contract to Huawei for the Mandalay smart city CCTV surveillance system without a tender process. The justification for the lack of a tender process was based on tender Directive No. 1/2017 without citing any specific article. No tender was called as the project was considered to be in the public interest and required a huge investment, and because Huawei had already been internally accredited.[83] Apart from having no legal basis, this also violates Myanmar's obligations under the UN Convention against Corruption, which the country signed and ratified.[84] Under the Convention, Article 9 requires 'public distribution of information relating to procurement procedures and contracts, including information on invitations to tender and relevant pertinent information on the award of contracts, allowing potential tenderers sufficient time to prepare and submit their tenders' and 'establishment, in advance, of conditions for participation, including selection and award criteria and tendering rules, and their publication', and finally 'use of objective and predetermined criteria for public procurement decisions, to facilitate the subsequent verification of the correct application of the rules or procedures'.

This expedited process was implemented arbitrarily by the government – Directive No. 1/2017 does not carve out any such exceptions. Given that the

CCTV surveillance system project is reportedly expected to cost around MMK 1.9 billion (about USD 1.25 million),[85] the project falls under Directive No. 1/2017 Article 10(c) which requires the tender to be announced at least twice in state-owned newspapers one month before the tender opening date, on relevant department's notice boards and, if possible, on the ministry's website. However, these requirements were not met. The lack of information published on the procurement process for this project highlights the opaqueness of the decision-making process in deploying CCTV systems.

While tenders for projects related to purchasing office furniture, printers, and the construction of buildings are somewhat transparent and publicised, various government departments or the ministries in Myanmar have traditionally selected a handful of companies to implement certain projects such as e-government-related initiatives, including GPS tracking systems and CCTVs. A source close to Naung Yoe Technologies disclosed that the company hired former generals, which resulted in the company winning tenders for government projects, including the installation of Naypyidaw CCTV networks and the command-and-control centre.[86] These companies normally include those that have little to no credibility, as well as military-owned companies or those that have close relationships with the government. For interested individuals or companies other than those who enjoy favour with the government, applicants must submit their company registration to enquire further about the tender.

From observation of the various call for tenders, it is common for ministries to apply different strategies for projects considered sensitive, such as those using surveillance technologies. For these particular projects, the government has either not announced projects or used broad, vague, or incomprehensible language in tenders.[87]

Most ministries do not publish when tenders had been awarded and keep information about military-linked companies implementing government projects with military-related companies away from public scrutiny. This information would only arise from investigative journalism or leaked documents.[88] As mentioned earlier, Myanmar does not currently have

an access to information legislation that can be used to gather more information. A Right to Information Bill was proposed in 2016 but has not been passed as of June 2022.[89] At the time of writing, the challenges to access information will not likely change, but rather will be exacerbated under military rule. Given the lack of information on which specific companies have been assigned to a specific tender, this research focused on those companies that are known to be involved in deploying CCTV networks in Mandalay and other major cities in Myanmar.

Technologies of interest: Tenders

Eleven tenders were analysed based on calls for tenders in 2020 to install and implement CCTV networks (see Table 1). Data was obtained from leaked tenders that were subsequently published online.[90] Tenders included the installation of CCTV networks in public spaces including the Mandalay University of Foreign Languages, six townships in Mandalay, the Yangon–Mandalay Highway, and various townships in Yangon, Sagaing, and Naypyidaw.

Police stand in front of blockades barring people from protesting on Pyidaungsu Yeithka Road, Yangon, Myanmar. **Photo:** February 2021, Digital Rights Collective.

Table 1: List of tenders reviewed[91]

Date of tender publication	Equipment	Locations	Responsible departments
1 April 2020	CCTV	Bam Mout; Yay Oo	Sagaing Regional Government
2 April 2020	49 pieces of CCTV installation and related components at City Hall and at the gates of the housing compound	City Hall, and housing compound	Engineering Department (Buildings), Naypyidaw Development Committee
15 May 2020	CCTV; AI; system and server (Safe City); Swiss challenge	Mahar Aung Myay; Chan Mya Thar Si; Pyi Gyi Ta Gon	Mandalay Regional Government
18 May 2020	7 locations and 3 control rooms with LCD monitors	Yangon–Mandalay Highway in Hlegu	Yangon Regional Police Office
19 June 2020	120 CCTV cameras and 2 monitoring control rooms (16 LCDs)	8 ports and 9 bridges along Yangon River	Myanmar Maritime Police Force and the Ministry of Home Affairs
1 July 2020	Individual loop sensor traffic point and traffic-light installation with computer system and CCTV cameras	6 townships in Mandalay	Mandalay City Development Committee and the Building and Central Store Department
10 July 2020	CCTV cameras	9 territories within Yangon Region	Yangon Region Police Force (using money from the Yangon Regional Government)
23 July 2020	CCTV and related equipment for command-and-control centre	Monywa Township	Sagaing Regional Government
27 July 2020	CCTV and generators	Mandalay University of Foreign Languages	Mandalay University of Foreign Languages and the Ministry of Education
3 December 2020	CCTV	Hmawbi Township	Yangon City Development Committee
17 December 2020	52-feet video wall display for Yangon Electricity Supply Corporation Control Room	Yangon	Ministry of Electricity and Energy

In addition to installing CCTV networks, several tenders also looked to implement monitoring control rooms (where police can monitor and analyse CCTV feeds) for the Yangon–Mandalay Highway in Hlegu, and the ports and bridges along the Yangon River. The implementing authorities of these control rooms are the Ministry of Home Affairs and the police, meaning that surveillance of civilians and their data (including biometric data) will be carried out by both the police and military. Departments responsible for the projects such as the Ministry of Home Affairs and the regional police departments provided little background information to the tender. An examination of the department websites where tenders were published also showed little information to contextualise the CCTV installation. The tenders analysed did not provide constructive information and the requirements used language that was vague and broad. For instance, the tender talks about needing 'necessary equipment' and 'security-related equipment', without any justification for what qualifies as 'necessary', and also without clarifying what purposes such equipment was 'necessary' for. Instead, it reads more like an open-ended category of technologies that may be unilaterally declared as 'necessary' at any given point in time. Specifications of what and why the technologies were needed were also not mentioned within the tenders. Further, the tender documents did not disclose the specific locations where CCTVs would be installed, nor did they provide information regarding the purpose or scope of these installations.

Figure 1 shows a document from the Ministry of Home Affairs, Police Force, and Prison Department in June 2021 as an example of a typical open tender. The tender stated that it was looking for necessary equipment, security-related equipment, inspection equipment, equipment for offices, furniture for offices, vehicles for offices, and other office-related equipment. The document also provided the deadline of the tender and the contact information. There is neither any background or contextual information, nor any justification or mention of the purpose of the required equipment. While they might be mentioned in confidential internal government documents, the equipment that is purchased as a result of the tender can only be found through investigative journalism or leaked documents.[92] Given the broad scope of information covered and the high penalties that can be imposed under the Official Secrets Act (1923), inside sources and journalists are in grave danger if they release the information.

ပြည်ထဲရေးဝန်ကြီးဌာန
စက်နှင့်စက်ပစ္စည်းဝယ်ယူမှုစီစစ်ရေးကော်မတီ
အိတ်ဖွင့်တင်ဒါ Open Tender ခေါ်ယူခြင်း

၁။ ပြည်ထဲရေးဝန်ကြီးဌာန၊ စက်နှင့်စက်ပစ္စည်းဝယ်ယူမှုစီစစ်ရေးကော်မတီသည် အောက်ဖော်ပြပါ တပ်ဖွဲ့/ဦးစီးဌာနများအတွက် လိုအပ်သောစက်နှင့်စက်ပစ္စည်းများ၊ လုံခြုံရေးသုံးပစ္စည်းများ၊ စစ်ဆေးရေး ပစ္စည်းများ ရုံးသုံးစက်ကိရိယာများ၊ ရုံးသုံးပရိဘောဂများ၊ ရုံးသုံးယာဉ်နှင့် အခြားရုံးသုံးပစ္စည်းများ၊ ဝယ်ယူရန်ရှိပါသဖြင့် ပြည်တွင်းမြန်မာနိုင်ငံသား ပုဂ္ဂလိကလုပ်ငန်းရှင်များအား အိတ်ဖွင့်တင်ဒါတင်သွင်း နိုင်ရန် ဖိတ်ခေါ်အပ်ပါသည်။

၂။ အဆိုပါပစ္စည်းတင်သွင်းလိုသော ပြည်တွင်းမြန်မာနိုင်ငံသား ပုဂ္ဂလိကလုပ်ငန်းရှင်များသည် တင်ဒါအဆိုပြုလွှာများကို ၁-၆-၂၀၂၁ ရက်နေ့မှစ၍ နေပြည်တော် ပြည်ထဲရေးဝန်ကြီးဌာန၊ ဝန်ကြီးရုံး၊ သက်ဆိုင်ရာ တပ်ဖွဲ့/ဦးစီးဌာနများတွင် ဝယ်ယူနိုင်ပြီး ၁၄ -၆ -၂၀၂၁ ရက်နေ့ ညနေ (၁၆၀၀)နာရီ နောက်ဆုံးထား၍ ပြန်လည်တင်သွင်းရမည်ဖြစ်ပါသည်။ လုပ်ငန်းရှင်များသည် တင်ဒါ အဆိုပြုလွှာအား သတ်မှတ်ထားသော စည်းကမ်းချက်များနှင့်အညီ ပြန်လည်တင်သွင်းရမည်ဖြစ်ပါသည်။

၃။ တင်ဒါဖွင့်လှစ်မည့်နေ့ရက်အား နိုင်ငံပိုင်သတင်းစာများမှ ထပ်မံကြော်ငြာမည်ဖြစ်ပါသည်။

၄။ အသေးစိတ်အချက်အလက်များ သိရှိလိုပါက အောက်ပါတယ်လီဖုန်းနံပါတ်များသို့ ဆက်သွယ် စုံစမ်းနိုင်ပါသည်-

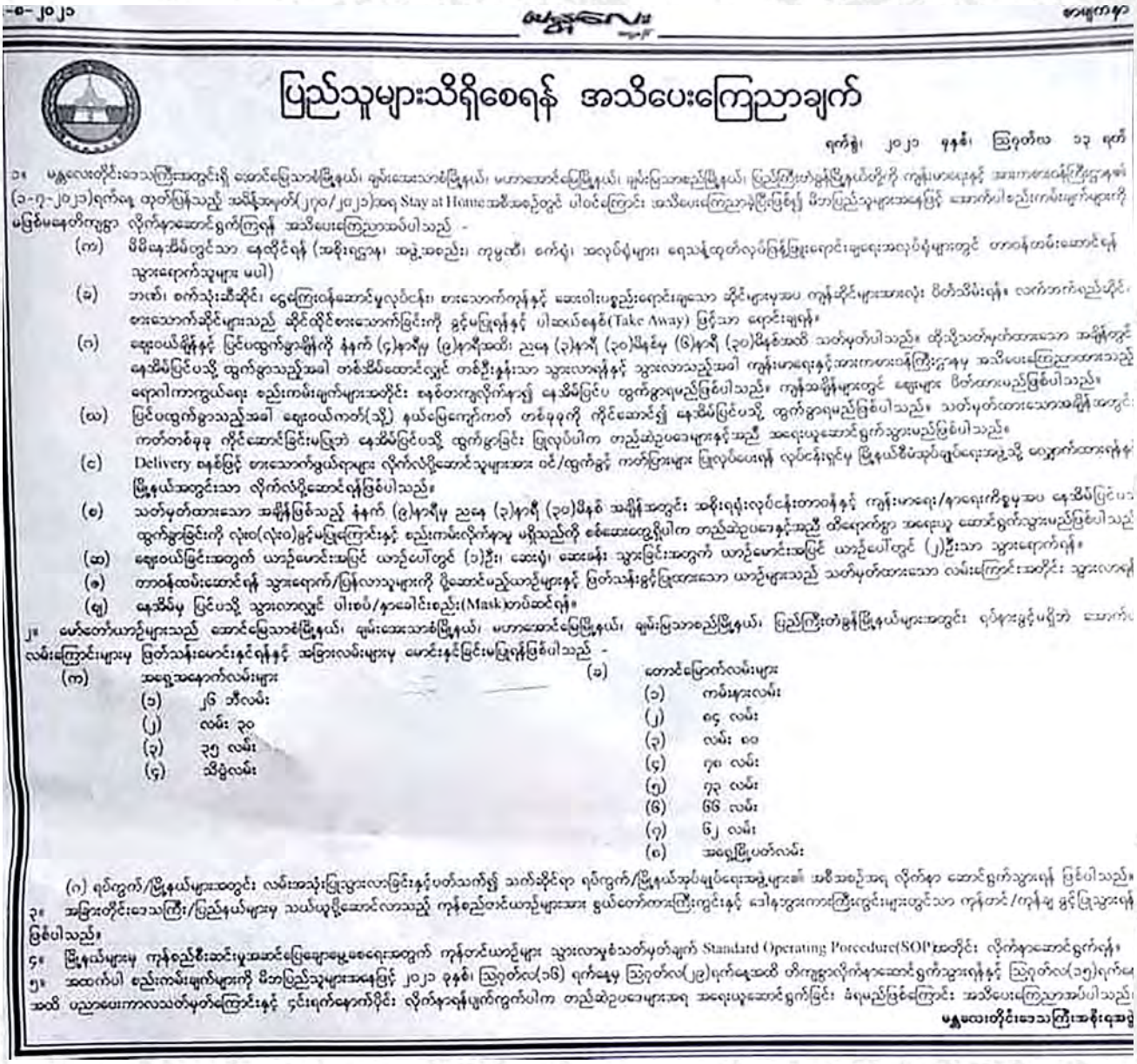
(က) ပြည်ထဲရေးဝန်ကြီးဌာန၊ ဝန်ကြီးရုံး ဖုန်း-၀၆၇-၃၄၁၄၄၆၆၊ ၀၆၇- ၃၄၁၄၇၈၈
(ခ) မြန်မာနိုင်ငံရဲတပ်ဖွဲ့ ဖုန်း-၀၆၇-၃၄၁၅၅၁၊ ၀၆၇- ၃၄၁၄၄၀၂
(ဂ) အကျဉ်းဦးစီးဌာန ဖုန်း-၀၆၇-၃၄၃၁၄၂၆၊ ၀၆၇-၃၄၃၁၄၂၀

စက်နှင့်စက်ပစ္စည်းဝယ်ယူမှုစီစစ်ရေးကော်မတီ

Figure 1: An open tender document from the Ministry of Home Affairs, Police Force, and Prison Department in June 2021 to supply equipment

Since the coup, some government entities currently under the control of the military have released calls for tenders on websites such as the Myanmar National Portal, and the relevant ministries' websites.[93] From the table of tenders, the Yangon Region Police Force and other government departments were to heavily equip Mandalay, Monywa, and Yangon and its outskirts with CCTVs starting from the second quarter of 2020, one year ahead of the coup. Under Mandalay's Safe City Project, the Mandalay Regional Government released a tender through a Swiss challenge to install CCTV, AI, and systems and servers for Mahar Aung Myay, Chan Mya Thar Si, and Pyi Gyi Ta Gon townships on 15 May 2020 (see Figure 2). Since the coup, these townships have been under high surveillance from the military due to their active participation in Myanmar's Civil Disobedience Movement.[94] The areas were given 'Stay at Home' orders by the current military-controlled Mandalay Regional Government following an intense crackdown on protesters in Mahar Aung Myay.[95] Fears about the junta police forces getting access to CCTV footage have led individuals from the movements to distribute pamphlets requesting households to take down or paint over CCTV cameras installed on their compounds.[96]

The push for CCTV installations in these specific townships is concerning as it is unclear which departments or individuals within the Mandalay Regional Government are leading the installation projects. With the majority of the Mandalay Regional Government staff on strike and the former mayor leading the Smart City Project detained since the coup, the lack of transparency about the department responsible and accountable to the public procurement process raises questions regarding the motives behind these post-coup projects.



ပြည်သူများသိရှိစေရန် အသိပေးကြေညာချက်

ရက်စွဲ၊ ၂၀၂၁ ခုနှစ်၊ ဩဂုတ်လ ၁၃ ရက်

၁။ မန္တလေးတိုင်းဒေသကြီးအတွင်းရှိ ဇောင်မြေသာစံမြို့နယ်၊ ချမ်းသာသာစံမြို့နယ်၊ မဟာဆောင်မြေမြို့နယ်၊ ချမ်းမြသာစည်မြို့နယ်၊ ပြည်ကြီးတန်ခိုးမြို့နယ်တို့တွင် ကျန်းမာရေးနှင့် အားကာကွယ်ရေးကြီးကြပ်ရေးအဖွဲ့ (၁-၇-၂၀၂၁)ရက်နေ့ တုတ်ပြန်သည့် အမိန့်အမှတ်(၂၇၀/၂၀၂၁)အရ Stay at Home အစီအစဉ်တွင် ပါဝင်ကြောင်း အသိပေးကြေညာခဲ့ပြီးဖြစ်၍ မိဘပြည်သူများအနေဖြင့် အောက်ပါစည်းကမ်းများကို မဖြစ်မနေတိကျစွာ လိုက်နာဆောင်ရွက်ကြရန် အသိပေးကြေညာအပ်ပါသည် -

(က) မိမိနေအိမ်တွင်သာ နေထိုင်ရန် (အစိုးရဌာန၊ အဖွဲ့အစည်း၊ ကုမ္ပဏီ၊ စက်ရုံ၊ အလုပ်ရုံများ၊ ရေသန့်ထုတ်လုပ်ဖြန့်ဖြူးရောင်းချရေးအလုပ်ရုံများတွင် တာဝန်ကျမီးဆောင်ရန် သွားရောက်သူများ မပါ)

(ခ) ဘဏ်၊ စက်သုံးဆီဆိုင်၊ ဂြေကြေးငန်ဆောင်မှုလုပ်ငန်း၊ စားသောက်ကုန်နှင့် ဆေးဝါးပစ္စည်းရောင်းချသော ဆိုင်များမှအပ ကျန်ဆိုင်များအားလုံး ပိတ်သိမ်းရန်။ သောက်ဘက်ရည်ဆိုင်၊ စားသောက်ဆိုင်များသည် ဆိုင်ထိုင်စားသောက်ခြင်းကို ခွင့်မပြုရန်နှင့် ပါဆယ်နေစဉ်(Take Away) ဖြင့်သာ ရောင်းချရန်။

(ဂ) ဈေးဝယ်ဖို့နှင့် ပြင်ပထွက်ခွာဖို့ကို နံနက် (၄)နာရီမှ (၉)နာရီထိ၊ ညနေ (၃)နာရီ (၃၀)မိနစ်မှ (၆)နာရီ (၃၀)မိနစ်အထိ သတ်မှတ်ပါသည်။ ထိုးဖိုသတ်မှတ်အားသော အဖြို့အတွင် နေအိမ်ပြင်ပသို့ ထွက်ခွာသည့်အခါ တစ်အိမ်ဆောင်လျှင် တစ်ဦးနှုန်းသာ သွားလာရန်နှင့် သွားလာသည့်အခါ ကျန်းမာရေးနှင့်အားကာကွယ်ကြီးကြပ်ရေးနှင့် အသိပေးကြေညာထားသည့် ရောဂါကာကွယ်ရေး စည်းကမ်းဖျက်များအတိုင်း စနစ်တကျလိုက်နာ၍ နေအိမ်ပြင်ပ ထွက်ခွာရမည်ဖြစ်ပါသည်။ ကျန်အဖြို့များတွင် ဈေးများ ပိတ်ထားမည်ဖြစ်ပါသည်။

(ဃ) ပြင်ပထွက်ခွာသည့်အခါ ဈေးဝယ်ကတ်(သို့) နယ်ပြေကျော်ကတ် တစ်ခုခုကို ကိုင်ဆောင်၍ နေအိမ်ပြင်ပသို့ ထွက်ခွာရမည်ဖြစ်ပါသည်။ သတ်မှတ်ထားသောအဖြို့အတွင် ကတ်တစ်ခုခု ကိုင်ဆောင်ခြင်းမပြုဘဲ နေအိမ်ပြင်ပသို့ ထွက်ခွာခြင်း ပြုလုပ်ပါက တည်ဆဲဥပဒေများနှင့်အညီ အရေးယူဆောင်ရွက်သွားမည်ဖြစ်ပါသည်။

(င) Delivery ဧနှစ်ဖြင့် စားသောက်ဖွယ်ရာများ လိုက်လံပို့ဆောင်သူများအား ဝင်/ထွက်ခွင့် ကတ်ပြားများ ပြုလုပ်ပေးရန် လုပ်ငန်းလှုပ်မှ ပြီနယ်စီမံအုပ်ချုပ်ရေးအဖွဲ့သို့ မေတ္တာရပ်ခံထားရန်နှင့် ပြီနယ်အတွင်းသာ လိုက်လံပို့ဆောင်ရန်ဖြစ်ပါသည်။

(စ) သတ်မှတ်ထားသော အဖြို့ဖြစ်သည့် နံနက် (၉)နာရီမှ ညနေ (၃)နာရီ (၃၀)မိနစ် အချိန်အတွင်း အစိုးရလုံးလုပ်ငန်းတာဝန်နှင့် ကျန်းမာရေး/နာရေးကိစ္စမှအပ နေအိမ်ပြင်ပသို့ ထွက်ခွာခြင်းကို လုံးဝ(လုံးဝ)ခွင့်မပြုကြောင်းနှင့် စည်းကမ်းလိုက်နာမှု မရှိသည်ကို စစ်ဆေးတွေ့ရှိပါက တည်ဆဲဥပဒေနှင့်အညီ တိုရောက်ခွာ အရေးယူ ဆောင်ရွက်သွားမည်ဖြစ်ပါသည်

(ဆ) ဈေးဝယ်ခြင်းအတွက် ယာဉ်မောင်းအပြင် ယာဉ်ပေါ်တွင် (၁)ဦး၊ ဆေးရုံ၊ ဆေးခန်း သွားခြင်းအတွက် ယာဉ်မောင်းအပြင် ယာဉ်ပေါ်တွင် (၂)ဦးသာ သွားရောက်ရန်။

(ဇ) တာဝန်ထမ်းဆောင်ရန် သွားရောက်/ပြန်လာသူများကို ဖွဲ့ဆောင်မည့်ယာဉ်များနှင့် ဖြတ်သန်းခွင့်ပြုထားသော ယာဉ်များသည် သတ်မှတ်ထားသော လမ်းကြောင်းအတိုင်း သွားလာရန်

(ဈ) နေအိမ်မှ ပြင်ပသို့ သွားလာလျှင် ပါးစပ်/နှာခေါင်းစည်း(Mask)တပ်ဆင်ရန်။

၂။ မော်တော်ယာဉ်များသည် ဇောင်မြေသာစံမြို့နယ်၊ ချမ်းသာသာစံမြို့နယ်၊ မဟာဆောင်မြေမြို့နယ်၊ ချမ်းမြသာစည်မြို့နယ်၊ ပြည်ကြီးတန်ခိုးမြို့နယ်များအတွင်း ရပ်များဖွင့်မရှိဘဲ အောက်ပါ လမ်းကြောင်းများမှ ဖြတ်သန်းမောင်းနှင်ရန်နှင့် အခြားလမ်းများမှ မောင်းနှင်ခြင်းမပြုရန်ဖြစ်ပါသည် -

(က) အရှေ့အနောက်လမ်းများ
- (၁) ၂၆ ဘီလမ်း
- (၂) လမ်း ၃၀
- (၃) ၃၅ လမ်း
- (၄) သီဖူလမ်း

(ခ) တောင်မြောက်လမ်းများ
- (၁) ကမ်းနားလမ်း
- (၂) ၈၄ လမ်း
- (၃) လမ်း ၈၀
- (၄) ၇၈ လမ်း
- (၅) ၇၃ လမ်း
- (၆) ၆၆ လမ်း
- (၇) ၆၂ လမ်း
- (၈) အလျှပြုပတ်လမ်း

(ဂ) ရပ်တွက်/ပြီနယ်များဆွတ်၊ လမ်းအသုံးပြုသွားလာခြင်းနှင့်ပတ်သက်၍ သက်ဆိုင်ရာ ရပ်ကွက်/ပြီနယ်အုပ်ချုပ်ရေးအဖွဲ့များ၏ အစီအစဉ်အရ လိုက်နာ ဆောင်ရွက်သွားရန် ဖြစ်ပါသည်။

၃။ အခြားတိုင်းဒေသကြီး/ပြည်နယ်များမှ သယ်ယူပို့ဆောင်လာသည့် ကုန်စည်တင်ယာဉ်များအား နယ်တော်ကာကြီးကွင်းနှင့် ဒေါနွားကာကြီးကွင်းများတွင်သာ ကုန်တင်/ကုန်ချ ခွင့်ပြုသွားရန် ဖြစ်ပါသည်။

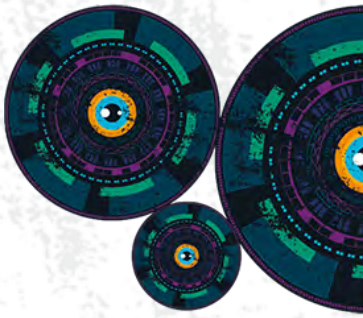
၄။ ပြီနယ်များမှ ကုန်စည်စီးဆင်းမှုအဆင်ပြေချောမွေ့စေရေးအတွက် ကုန်တင်ယာဉ်များ သွားလာမှုစံသတ်မှတ်ချက် Standard Operating Porcedure(SOP)အတိုင်း လိုက်နာဆောင်ရွက်ရန်။

၅။ အထက်ပါ စည်းကမ်းဖျက်များကို မိတပြည်သူများအနေဖြင့် ၂၀၂၁ ခုနှစ်၊ ဩဂုတ်လ(၁၆) ရက်နေ့မှ ဩဂုတ်လ(၂၉)ရက်နေ့အထိ တိကျစွာလိုက်နာဆောင်ရွက်သွားရန်နှင့် ဩဂုတ်လ(၁၅)ရက်နေ့ အထိ ပညာဗေးကာလသတ်မှတ်ကြောင်းနှင့် ၄င်းရက်နောက်ပိုင်း လိုက်နာလုံမှုကိုကွပ်ပါက တည်ဆဲဥပဒေများအရ အရေးယူဆောင်ရွက်ခြင်း ခံရမည်ဖြစ်ကြောင်း အသိပေးကြေညာအပ်ပါသည်။

မန္တလေးတိုင်းဒေသကြီးအစိုးရအဖွဲ့

Figure 2: Clipping from the Mandalay newspaper regarding the 'Stay at Home' for Aung Myay Thar Zan, Chan Mya Thar Si, Mahar Aung Myay, and Pyi Gyi Ta Gon townships, released on 13 August 2021

Who builds and supplies this technology?



Different companies play the role of vendor and implementer within Myanmar's smart cities. Vendors provide the infrastructure and technology, while implementers purchase, install, and operate systems. In Yangon and Naypyidaw, even though local companies were selected to implement CCTV systems, all were found to have purchased CCTV equipment from Huawei.[97] This process was reversed in Mandalay whereby Huawei won the tender directly to sell their products, while two local companies, Ace and Zarni Electronics, were assigned to implement the installation.[98] Little information was found about the two local companies while conducting the research. Nonetheless, the available information shows that the vast majority of the infrastructure is provided by the same actor, i.e. Huawei. Given the integrated nature of CCTV footage, it is also necessary to ask which companies beyond Huawei form part of the mix in terms of maintaining equipment, repairs, ensuring smooth software upgrades and solving related issues, and training police and military staff to operate these systems, etc.

> "Regardless of the procurement process used, ARTICLE 19 and Digital Rights Collective have found that Huawei equipment was ultimately deployed irrespective of the implementing company. Huawei has an almost universal presence in providing basic equipment."

While Mandalay's CCTV contract with Huawei during the NLD government term made headlines, there was relatively less public awareness of Naypyidaw's bigger and earlier CCTV installation project. The city

mandated Naung Yoe Technologies and Linn IT Solution, two companies founded by former military generals, to implement CCTV installation. Naung Yoe Technologies is also known for helping the military during military rule before 2011.[99] In 2014, a leaked email revealed that Naung Yoe Technologies sent enquiries to the Italian surveillance malware vendor Hacking Team, expressing interest in an interception system for mobile devices on behalf of the Ministry of Defense.[100] The structural construction and implementation of the system influences how it will be used and can present weaknesses which can be abused. These companies can decide on the infrastructure where certain entities could be allowed to gain access to sensitive personal data of political dissidents, protesters, and other individuals and communities deemed to be troublesome to the military, with or without public awareness.

Another company that Myanmar authorities have historically selected to implement CCTV systems is MySpace International, a company led by ex-military officers. MySpace International handled the purchase of Cellebrite – the notorious mobile data extraction tool, also known as a mobile device forensic tool – that has been used by governments around the world, including in Myanmar, to target human rights defenders, journalists, and activists.[101] For instance, Cellebrite was used by the Myanmar police against two Reuters journalists, Wa Lone and Kyaw Soe Oo, who reported on atrocities against the country's Rohingya Muslim minority. They were sentenced to seven years for violating the Official Secrets Act (1923) using the information extracted from their mobile phones.[102] Government agencies increasingly rely on technology companies to assist in the acquisition of sensitive technologies or equipment.

FISCA was also another company found to be implementing CCTV systems.[103] After the military coup, the junta pushed to implement the same project in Mawlamyine, where the military-tied companies Naung Yoe Technologies and FISCA, who oversaw the installation in Naypyidaw and Yangon, respectively, were permitted to implement the project.[104]

From our analysis, regardless of the procurement process used, the same outcome (using Huawei equipment) was reached and was ultimately deployed irrespective of the implementing company. Furthermore, it makes

no difference in how the two regional governments mandated companies to install CCTVs in Yangon and Naypyidaw – both the NLD government and the military have given permission to a select few companies that have close military ties or were founded by retired former generals. This is likely to have helped the military junta gain relatively easier access to the infrastructure and to continue pushing the project with the same companies. It is apparent from the Mawlamyine example that the junta has allowed the same companies within their influence to work on the new projects. It also shows that Huawei has an almost universal presence in providing basic equipment.

> "For the Myanmar government, decisions to purchase systems and equipment are solely based on cost rather than on safeguards for people's rights."

Throughout our interviews, civil society expressed that the government will, by default, opt for cheaper options, such as Huawei, regardless of privacy considerations.[105] Indeed, for the Myanmar Government under the NLD, the decision on purchasing the systems and equipment solely based on cost rather than on safeguards for human rights seemed the chosen approach. High-tech CCTVs (such as those equipped with face recognition) are not the only Huawei products potentially encroaching on public space in the county; Huawei has also offered many aspects of digital integration in Myanmar's transformation from banking[106] to cloud services.[107]

Critical gaps in information

Equipment specifications

Given that information on published tenders includes vague language and only mentions CCTVs or control room monitors, it can be difficult to acquire information about specific CCTV equipment that successful companies are required to provide. This is an observation based on an analysis of the leaked tenders that were published online (see earlier). For example, the Yangon Region Police Force called for tenders to deploy CCTVs in nine territories within the Yangon Region. However, they did not include detailed technical specifications for the CCTVs. There has been no public information from the government on how the technology[108] works and how the data will be handled by the departments during the NLD government.

While we do not know about specific equipment acquired, we do know that Huawei CCTVs are the predominant choice for devices in installations.[109] However, we do not know what capabilities these systems have, particularly in relation to detecting faces and vehicles' licence plates. There are different types of CCTV cameras that Huawei offers to clients and one of the highlights is a software-defined camera. According to their website,[110] there are three main series of software-defined cameras: the X (eXtra) series, the M (Magic) series, and the C (Credible) series. All of these are equipped with advanced AI chips. According to the Huawei Intelligent Video & Data Analytics iCAN Evaluation Criterion White Paper, it seems that Huawei is pushing for 'one cloud for the whole region' wherein video images will be integrated with multi-dimensional data and shared across domains and systems.[111] The paper also stressed the need to develop a unified video and data analytics intelligence evaluation system as a guide and reference. Software-defined intelligence will use traditional CCTVs for the implementation of intelligent transformation. The information regarding which type of system the regional governments used is unknown.

"CCTVs are quickly becoming ubiquitous across Myanmar – placed at traffic lights, landmarks, universities, city halls, municipal buildings, parliament buildings, and embassies. Because they collect highly sensitive personal data they bring up a host of data protection concerns. In the absence of data protection laws that adequately regulate the collection, use, transfer, and retention of this data, the use of these systems provides powerful entities with carte blanche on how to analyse, use, and retain personal information."

Extent and progress of CCTV installation

As of July 2022, there has not been any update released on the progress of CCTV installations in the three neighbourhoods in Mandalay or on the surveillance project in Hlaing Thar Yar. It is crucial to know how these two neighbourhood CCTV projects are different from Naypyidaw's citywide, fully operational CCTV networks, as the current lack of information about placement, procurement, and use of CCTV cameras paints a hazy picture (at best) of how Myanmar's surveillance network is growing. This is also an important area of research and analysis for civil society, as understanding the similarities and differences between the two would help determine how to ultimately demand the removal of these cameras. Apart from the number of CCTVs, which we learnt from media reports, we do not know the locations in which CCTVs will be installed; specific locations such as street corners, inside neighbourhood streets, or in crowded places would shed light on the government's attempts to control 'crime' and how it can infringe human rights. For example, in Hlaing Thar Yar, there are 140 cameras for a township of 67.4 km^2 and so we assumed that there will be one CCTV per 0.5 km^2, or that cameras would be concentrated in particular areas, such as on streets near factory workers' residences.

Chain of control and oversight

Based on the calls for tenders, it also seems that different government departments such as the police force, city development committees, electricity supply offices, engineering departments, regional government offices, and the Ministry of Home Affairs are handling different projects in different areas and it is not clear how they will be interconnected – if at all – after the projects are implemented. For example, will there be centralised access to the police department, or will they fall under the management of a particular ministry? It is not clear how many control centres there will be or if they will all be centralised, or how different police departments will coordinate. During the NLD government's tenure, our interviewees informed us that the budgets for smart city projects were either allocated by the Myanmar Government or provided by each

regional government from their own municipal budget or taxation. It is unclear how or if different government ministries or departments coordinate in such projects; interviews with civil society working closely with the government said different ministries under NLD were inconsistent in their approaches to the implementation. It is likely that under the NLD government, different surveillance projects were run separately under different department policies. Investigating how this is likely to change under the military junta is an important area of research, as knowing the distribution of responsibility and budgets will serve as a starting point for civil society to scrutinise procurement and use of these systems, and it will also enable tapping into accountability processes surrounding the use of CCTVs. And yet, even under the NLD government, there was a complete lack of a comprehensive regulatory framework for data protection and privacy applicable for different departments – and little interest in adopting one.

"Evidence of how data in current cases is handled in Myanmar does not inspire confidence but reveals a modus operandi that does not consider the importance of privacy and data protection. In an unsolved case of child sexual assault, the police department unnecessarily released the child's identity on social media, without providing her any prior warning or obtaining her consent."

Nature of current use

Because of the lack of transparency, proactive disclosure, and avenues for access to information, details of current use and exact responsibilities are yet to be uncovered. This opacity is at odds with international standards of transparency and responsible public procurement (see Right of Access to Information). Concerns about transparency are even more urgent given the military's control of public infrastructure, whereby smart city systems such as CCTV networks are readily used to monitor protests and other dissidents. Since the time of the

NLD government, tender documents showed that different government departments have regularly contracted private companies for CCTV installations in places such as traffic lights, landmarks, universities, city halls, municipal buildings, parliament buildings, and embassies in Yangon, Mandalay, Naypyidaw, and Monywa. By 2020, the command-and-control centres (the centres equipped with surveillance systems and monitors that enable the police to view and analyse CCTV footage) had already been built in these four cities. While the city-related installations came from individual regional governments, calls for installations coming from the police force were generally under the command of the Ministry of Home Affairs, a ministry that had always been under the direct influence/control of the military,[112] even during the NLD government. Leaked documents show that after the coup, the military junta has been ramping up efforts to extend the remaining projects in cities like Mandalay and Mawlamyine.[113]

Finally, it is unclear how the individual governments envisioned CCTV installations as part of the smart city plan or general development in their narratives. At the end of the day, however, **all** CCTV networks contribute to an overarching surveillance system in Myanmar. Different regional governments have designed their safe city projects under the umbrella of the smart city, which involved the installation of CCTVs in their chosen civilian neighbourhoods to monitor crime reduction; however, other camera installations, such as Yangon's vast network of traffic light CCTVs or Naypyidaw's citywide CCTVs, did not fall under the smart city narrative.

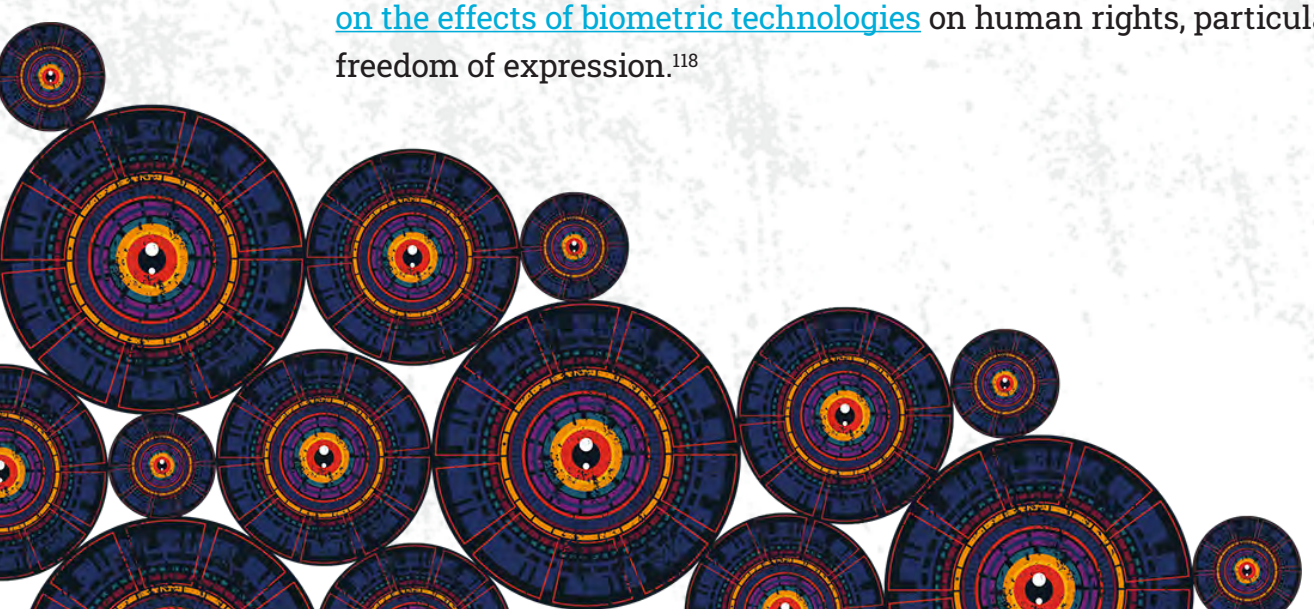
On CCTV systems and human rights

The deployment of CCTV cameras, both traditional and AI-enabled, affects people's ability to exercise a number of human rights. The Universal Declaration of Human Rights (UDHR)[114] protects individuals' human rights, and the International Covenant on Civil and Political Rights (ICCPR)[115] gives them legal force. The UDHR's provisions are incorporated into customary international law, making it binding on all states.

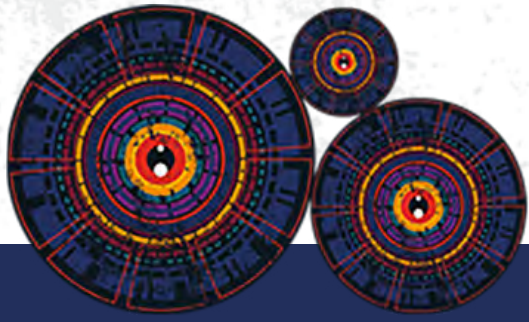
Myanmar has not yet ratified the ICCPR. However, under customary international law, states are under binding legal obligations to promote, respect, protect, and guarantee human rights. Private companies also have the responsibility to respect human rights, as envisioned in the UN's Guiding Principles on Business and Human Rights.[116] While these principles are not binding, the UN Special Rapporteur on freedom of opinion and expression has opined 'the companies' overwhelming role in public life globally argues strongly for their adoption and implementation'.[117]

The installation of CCTV cameras worldwide has demonstrated the grave implications these technologies have on the exercise of human rights. As discussed earlier in this report, these cameras collect personal data that brings up a host of data protection concerns, particularly worrying in jurisdictions with little to no regulation about the collection, use, transfer, and retention of personal data – like Myanmar.

When CCTV cameras include capabilities for biometric recognition, such as face and emotion recognition, the implications for human rights are even more worrying, as discussed in the Background. Risks arising from biometric technologies are covered in detail in ARTICLE 19's policy brief on the effects of biometric technologies on human rights, particularly the freedom of expression.[118]



Right to privacy



Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies, and other individuals.

The right to privacy is commonly recognised as a core right that underpins human dignity because it recognises the ability of individuals to control important areas of their own life, facilitates the development of their sense of self, allows for personal intimacy and family relationships. **Without privacy, individuals lack the space to think and reason and develop their own voice.** Privacy is a prerequisite to the meaningful exercise of free expression, given its role in preventing state and corporate surveillance.

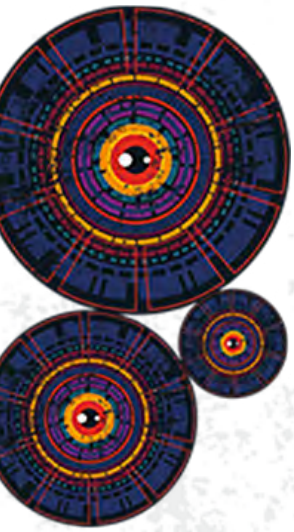
The right to anonymity is also seen as a vital part of the rights to expression and privacy. If biometric technologies are used to identify and profile people, they negate individuals' ability to communicate or move anonymously.

"Anonymity creates a zone of privacy to protect opinion and belief, which is especially crucial in hostile political, social, religious, and legal environments."

UN Special Rapporteur on freedom of opinion and expression

The **right to privacy** is guaranteed by Article 12 of the UDHR and Article 17 of the ICCPR and in regional treaties. While privacy (as well as the other human rights discussed in this section) is not an absolute right, it may be restricted only in very specific circumstances. Restrictions on privacy must meet the requirements of the **three-part test** of legality, necessity, and proportionality:

1. Restrictions must be provided by law that is sufficiently accessible, clear, and precise;
2. The restriction must be in pursuit of a legitimate aim; and
3. The restriction must be necessary, in proportion to the aim, and the least intrusive option available.[119]



In 2018, the UN Special Rapporteur on the right to privacy called into question the proportionality of biometric systems.[120]

International human rights bodies have also moved towards recognising a **right to anonymity** as an important aspect of the rights to freedom of expression and privacy.[121] If biometric technologies are used for identification or profiling purposes in public spaces, such as the use of CCTV cameras and facial recognition technologies to process facial images captured by video cameras on streets, squares, subways, stadiums, or concert halls, they negate individuals' ability to confidently communicate anonymously and have anonymity when moving and behaving in public spaces. As noted by the UN Special Rapporteur on freedom of opinion and

expression, anonymity "creates a zone of privacy to protect opinion and belief", which is especially crucial in "hostile political, social, religious and legal environments".[122] Hence, state interference with anonymity should be subject to the three-part test of legality, necessity, and proportionality, as is any other interference with this right.

In Myanmar, the right to privacy is violated by the widespread deployment of CCTV systems, particularly those collecting biometric data. In the absence of data protection laws that adequately regulate the collection use and storage of this data, the use of these systems provides powerful entities with carte blanche on how to analyse, use, and retain personal information. Evidence of how data in current cases is handled does not inspire confidence but rather speaks about a modus operandi that does not consider the importance of privacy and data protection. For example, in an unsolved case of child sexual assault, where the victim has become pseudonymously known as Victoria, the police department unnecessarily released the identity of the survivor on social media, without any prior warning or consent.[123]

Despite the NLD government's justification on safety, security, and crime reduction, which is discussed later, civil society participants also expressed concerns over trade-offs involved in the narrative around privacy versus crime safety, in the absence of an adequate legal framework, public consultation, and careful planning. For example, they voiced possible misuses of the data by the government and the lack of accountability and redressal in the case of faulty or arbitrary interpretation of data, wrongful convictions based on such data, and also concerns about authorities being racially biased (e.g. the authorities assuming that the riots or crimes are likely to happen near the mosques, which could reinforce racial profiling based on existing racial prejudices in Myanmar society). Given the corruption of some government ministries, data could be manipulated, it could mysteriously go 'missing', or police forces could withhold data – for example, there was unexplained missing CCTV footage in the murder case of the well-known NLD legal counsellor Ko Ni.[124]

Right to freedom of expression

Freedom of expression and privacy are mutually reinforcing rights. Privacy is a prerequisite to the meaningful exercise of freedom of expression, particularly given its role in preventing state and corporate surveillance that stifles free expression. Freedom of expression is fundamental to political dissent, diverse cultural expression, creativity, and innovation, as well as the development of one's personality through self-expression.

The **right to freedom of expression** is protected by Article 19 of the UDHR and given legal force through Article 19 of the ICCPR, as well as in regional human rights treaties. Under international human rights standards, restrictions on the right to freedom of expression are permitted only if they meet the three-part test of legality, necessity, and proportionality; all restrictions must be strictly and narrowly tailored and may not put the right itself in jeopardy.[125]

The installation of CCTV cameras as discussed in this report interferes with the freedom of expression in multiple ways. The politics of where these systems will be installed, and their intended use, introduce a new layer of political and social intimidation – neighbourhoods that are being 'watched' more closely will bear the brunt of the vicious cycle of over-policing.

Mass surveillance has a chilling effect on freedom of expression.[126] Studies show that the awareness of being watched and tracked might lead people not to join public assemblies, participate in social and cultural life, or freely express their thoughts, conscience, and religious beliefs in public spaces.[127] It also directly compels people to alter their behaviours – particularly in their political life – out of fear of being arrested, harassed, and otherwise singled out by repressive regimes. The intention of ubiquity and tracking implicit in Myanmar's current CCTV procurement discussed

in this report suggests that it is not consistent with the three-part test, particularly given the increasingly brutal crackdown against pushback, critique, and political speech in the country.

Right to freedom of peaceful assembly

The **right to freedom of peaceful assembly** is guaranteed in Article 20 para 1 of the UDHR and given force in Article 21 of the ICCPR, Article 5(d) of the International Convention on the Elimination of All Forms of Racial Discrimination and in regional treaties. Under these standards, requirements for a permissible restriction must comply with the same three-part test as for the restrictions on the right to freedom of expression and privacy.

The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association stated:

> "The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited. Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision."[128]

As evidenced through the findings of this report, Myanmar's current approach towards CCTV installation and use does not reflect this narrowly constructed view of surveillance and, to the contrary, perpetuates the idea of mass surveillance with a disproportionate impact on historically disadvantaged groups.

Progressive interpretation of the right to freedom of expression and the right to freedom of peaceful assembly leads to the recognition of the **right to protest**, which also includes the right to take part in the conduct of public affairs; the right to freedom of thought, conscience, and religion; the right to participation in cultural life; the rights to life, privacy, liberty, and security of a person; and the right to non-discrimination. The right to protest is also essential to securing all human rights, including economic, social, and cultural rights.[129]

States should ensure that derogable rights (qualified rights), which are integral to the right to protest, are subject to restrictions only on grounds specified in international law. In particular, no restriction on the rights to freedom of expression, assembly, association, or privacy may be imposed unless the restriction is provided by law and is legitimate, necessary, and proportionate.

Using facial recognition technologies during protests may discourage people from taking part in protests, which can have clear negative implications for the effective functioning of participatory democracy. Even if applied to police violence in protests, facial recognition may still affect peaceful protesters or bystanders. In other words, the deployment of facial recognition may generate a chilling effect whereby individuals alter their behaviour and refrain from exercising their rights to protest. People might thus be discouraged from meeting individuals or organisations, attending meetings, or taking part in certain demonstrations. Likewise, live facial recognition in public spaces can be used to target journalists, posing a chilling effect on individuals' and societies' access to information on protests. A plethora of examples from around the world demonstrate the tendency of states to use CCTV cameras and subsequent add-ons like face and emotion recognition to stifle the right to protest, expression, anonymity, and political speech.[130]

"A plethora of examples from around the world demonstrate the tendency of states to use CCTV cameras and facial recognition technologies to stifle the right to protest, expression, anonymity, and political speech. Such technologies are used to target journalists and dissidents, and can also affect peaceful protesters and bystanders. As a result they create a chilling effect on individuals and hamper the effective functioning of participatory democracy."

In Myanmar, facial recognition cameras are now being used to monitor and track people down.[131] In fact, the Myanmar population is well aware of the presence and dangers of watchful eyes on every corner in big cities such as Yangon, Mandalay, and Naypyidaw. Myanmar protesters in February and March 2021 took inspiration from the masked protesters from Hong Kong, and covered, or even destroyed, CCTVs in some areas during the protests. In October 2021, the youth resistance group spread pamphlets[132] in Yangon to request people to remove CCTV from their houses in case the junta police forces obtain the footage. When used along with CCTVs, facial recognition can prove a dangerous technology in helping the military find out the whereabouts of activists who are hiding. It is also worth noting that Naypyidaw, one of the most well-equipped cities in relation to surveillance systems, was the first city to quell protests during the early months of the uprising. It is reported[133] that the existing CCTVs helped the military identify and arrest protesters in Naypyidaw.

Right of access to information

"Several important details about Myanmar's CCTV network remain unknown. Equipment specifications, extent of current use, accountability mechanisms surrounding use and responsible authorities, for instance, are all unanswered questions."

The **right of access to information** is recognised as a key element of the right of freedom of expression in the UDHR and ICCPR. In 2011, the UN Human Rights Committee interpreted the scope of Article 19 of the ICCPR to include ensuring the right to information held by public bodies. It requires that states respond to requests for information and proactively disseminate information in the public interest and that the access is 'easy, prompt, effective and practical'.[134] The Human Rights Committee also laid down that states must enact 'necessary procedures'

"Given the transparency issues, it is likely that Myanmar's future network of smart cities will cement opacity and unilateral action as a feature of their structure, unless a right to information law is put in place, and accountability and transparency mechanisms are implemented."

such as adopting legislation to give effect to the right to information, and that fees for access must be limited, responses to requests must be timely, authorities must provide explanations for withholding information, and states need to establish appeals mechanisms. Right to Information laws, which have been adopted in around 130 countries, are powerful legal tools that individuals, journalists, and activists can use to improve government transparency and to understand the government's use of public funds and data.[135] They are also included in other international agreements, including Article 10 of the UN Convention against Corruption, which has been ratified by Myanmar, and SDG 16.10 of the UN Sustainable Development Goals.

Several important details about Myanmar's CCTV network remain unknown at the time of writing this report. Information about equipment specifications, extent of current use, accountability mechanisms surrounding use and responsible authorities, for instance, are unanswered questions. While our research uncovered some information about who is building this technology and the entities interested in buying it, there are still critical gaps in information required for meaningful engagement with government entities in Myanmar.

Given the transparency issues surrounding biometric technologies discussed earlier in this report, it is likely that Myanmar's future network of smart cities will cement opacity and unilateral action as a feature of their structure, unless a right to information law is put in place, and accountability and transparency mechanisms are implemented.

Right to non-discrimination and the right to equality

The **right to non-discrimination and the right to equality** is protected by Article 2 and Article 7 of the UDHR and is given legal force through Article 2 and 26 of the ICCPR, Article 2(2) of the International Covenant of the Economic, Social and Cultural Rights, as well as regional treaties and instruments. The right to equality implies that all persons are to be given 'equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'.

Interviewees mentioned their concerns about the increasing power differential between police officers and individuals afforded by the use of CCTVs. In Yangon, CCTVs were installed as a priority in 'high crime' areas like Hlaing Thar Yar, which is also home to some of the weaker socioeconomic communities in the city.[136] This indicates that CCTVs are more likely to be installed in neighbourhoods with poorer socioeconomic backgrounds, intensifying concerns around the concentration of power. Some interviewees even went so far as to suggest that the use of CCTVs could worsen how police forces harass and intimidate vulnerable and marginalised communities such as transgender people, who have been previously targeted with abuse from the Myanmar police.[137]

Disproportionate CCTV surveillance is not only likely to fall on weaker socioeconomic groups, but also ethnic and religious minorities in Myanmar given its track record in previous years. In 2017, Myanmar security forces perpetrated a campaign of violence against the Rohingya Muslim minority in Rakhine State which the UN High Commissioner for Human Rights called a 'textbook example of ethnic cleansing'.[138] The 2017 fact-finding mission found that there had been violence against minority groups, amounting to genocide and crimes against humanity, with the military primarily responsible.[139]

"In the absence of an adequate legal framework, public consultation, and careful planning, concerns around possible misuses of the data are also growing. These could include faulty interpretations of data, wrongful convictions based on such data, and racial bias, where authorities may assume that riots or crimes are likely to happen near mosques. Such assumptions reinforce racial profiling based on existing racial prejudices in Myanmar society. The right to equality implies that all persons are to be given 'equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Additional challenges

On the justification of 'safety'

Safety is the foremost justification used by authorities to exert excessive control and to put in place CCTV technologies across cities in Myanmar. These measures involve significant restrictions to the rights discussed earlier in this section, while at the same time failing to meet the three-part test.

Corruption within government ministries also leave room for data to be manipulated, to go mysteriously 'missing', or for the police to withhold data. For example, there was unexplained missing CCTV footage in the murder case of the well-known NLD legal counsellor Ko Ni.

The restrictions on rights do not have a legal basis and are reflective more of an executive whim. These practices are also neither necessary nor proportionate. To meet these standards, practices must not only be useful or desirable but also specific and necessary to achieve the scope, and there should be no other less intrusive ways to do so. There are multiple less intrusive ways to achieve the same result of 'safety' without breaching human rights in the manner that is currently normalised. If these tests are not met, the use of these technologies should not be allowed, irrespective of their availability or allure.[140]

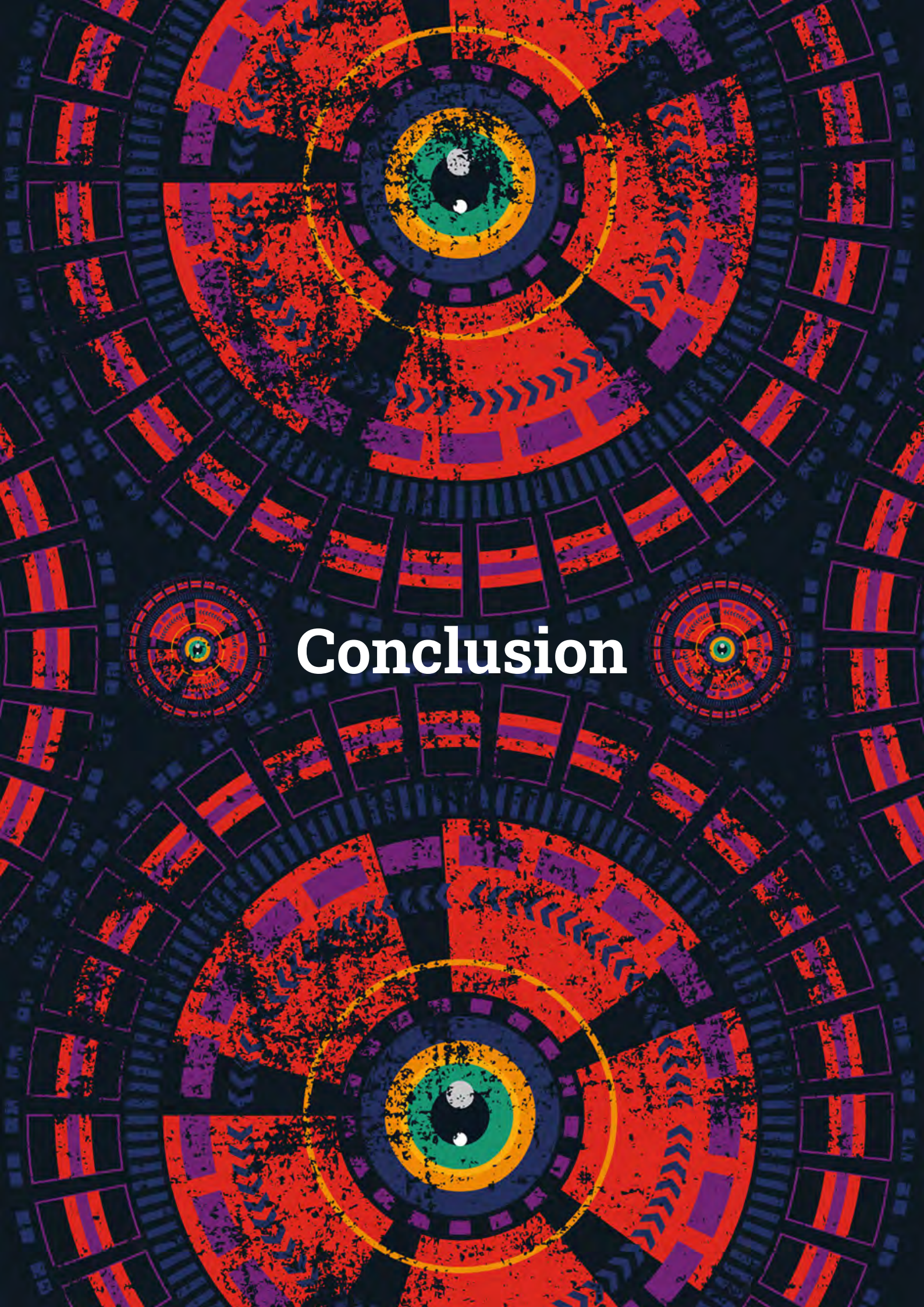
On the lack of transparency and public participation

Given the increasingly brutal crackdown against pushback, critique, and political speech, together with the intention of ubiquity and tracking implicit in Myanmar's current CCTV procurement, ARTICLE 19 believes that the authorities are failing in their duty to uphold this right for the people of Myanmar. The country's current approach towards CCTV installation perpetuates the idea of mass surveillance.

Despite the narrative of the NLD government to install AI-driven surveillance technology in big cities to provide 'safety' to the public, there was hardly any kind of public consultation on potential surveillance within broader smart city frameworks or consultations.[141] The question of a legitimate aim is important here. Even if safety concerns may be legitimate, their potential impact on human rights means that the deployment of CCTVs should be subject to scrutiny, public debate, and deliberation. But this is not the case in practice. High-level officials seem to have embraced a reliance on Chinese companies like Huawei and Dahua as a way to exacerbate existing practices, and also to impart new ones along the way.[142] As the government has been using various tracking systems – ranging from traditional phone tapping, special police, and car tracking to mandatory guest registrations – CCTV technology can and will readily assist such restrictive measures for the junta.

Mass surveillance has a chilling effect on people. The awareness of being watched and tracked prevents people from freely expressing thought or practising their religious beliefs in public spaces. It also compels people to alter their behaviours – particularly in their political life – out of fear of being harassed, hurt, or arrested.

What's worse, such surveillance has a disproportionate impact on historically disadvantaged groups including ethnic and religious minorities, and the poor.



Conclusion

We conducted this research to shed light on the visible structures and potential impacts of Mandalay's smart cities projects on human rights. In particular, we identified that CCTV projects in Myanmar's cities – whether they are under smart city projects or general city development – should be scrutinised to uncover possible risk areas. Our approach to this research is based on the axiom that surveillance technology can curb freedom of expression, privacy of movement, civil liberty, and civic participation, which is harmful for a democratic society. As there has been little prior public scrutiny on smart city projects in Myanmar, their surveillance systems, justified for 'crime reduction', are obscure under the umbrella of 'smart city' plans.

A few important threads emerged from our research which should be explicitly mentioned as a way of signposting future work to build on our report:

1. In Myanmar, particularly since the coup, CCTV cameras have become a kind of weapon that repressive forces have seized and are using to silence dissent. While the narrative of 'safety' encourages the purchase of these technologies, it is the ambition of surveillance and control that currently sustains it. The exact ways in which this power is wielded is an important question for civil society to explore, as is the question of how this impacts dissent across the country.

2. Private companies increasingly find cunning ways to obscure the extent of their involvement – or their involvement in smart cities altogether. This is an important pattern for civil society to look into for future work, particularly as it helps draw an accurate picture of the financial and technological concentration of power within smart cities.

3 The procurement process in Myanmar is evidently steeped in secrecy and nepotism, with little information about how to use, buy, and maintain technology available in the public domain. Tracing the routes of favouritism and understanding the extent of it can help explain which companies are primed to scale their products across Myanmar, and why. It is also important to document in further detail the lack of transparency and accountability in public procurement that lends itself to nepotism.

4 Even where procurement decisions are demonstrated and explained, there is still room for unilateral and arbitrary decisions, like the public interest exception which was used to circumvent the need for any tender process, in the absence of any provision of law enabling this exemption (see Public procurement process).

Students from Yangon Technological University organise a protest to denounce the military coup and call on civil servants to join the Civil Disobedience Movement in Yangon, Myanmar.
Photo: February 2021, Digital Rights Collective.

In particular, we hope that this work facilitates civil society and academic scrutiny about the process and nature of technology procurement within Myanmar's smart cities. Possible topics can include:

1. Further research into the process and nature of technology procurement within Myanmar's smart cities to find avenues for getting involved in shaping the process.

2. Further research on the critical gaps in information outlined in this report, specifically:

   a. What is the extent of the current CCTV use in Myanmar?

   b. What are the technical specifications of CCTVs currently being procured?

   c. Which government departments are responsible for the procurement, maintenance, use, and oversight of CCTVs?

   d. How do Myanmar's safe and smart city projects overlap?

   e. Does this overlap (or lack of) have any implications for funding, control, and use?

3. Documenting evidence of harm, or instances of arbitrary use of state power arising from the use of these systems.

It is apparent now, more than ever, that such technology has become a state tool to oppress pro-democracy movements under the newly formed military regime, with the junta tracking and cracking down on activists. Given the secrecy of the government and the institutions wielding the power to use such technology to watch over the people, it is difficult to prove the extent, underlying structure, or inner workings of the system. Our research shows that there are several information gaps in Myanmar CCTV networks at this time, especially as their use causes real harm to real people. The continuity with and heightening of prior repressive practices merit some attention and closer analysis, particularly of the technologies that facilitate this continuation.

Recommendations

A **rights-respecting framework for developing smart cities** in Myanmar would require:

1. **Banning mass surveillance** in public and publicly accessible spaces.

2. **Banning the design, development, and use of emotion recognition technologies.**

3. **Subjecting the design, development, deployment, and use of technologies** that impact human rights in the territory of Myanmar to the **strict tests of legality, necessity, and proportionality.**

4. **Placing a moratorium on the procurement and deployment of technologies** described in this report until there is adequate public debate on the implications of such systems on societies, and until adequate legislative safeguards are put in place.

5. **Putting in place accountability structures and independent oversight measures and a legislative framework** for the design, development, and deployment of CCTV and related infrastructures in compliance with international human rights standards.

6. **Putting in place comprehensive data protection legislation** in line with international law, and in consultation with a wide range of stakeholders, including civil society.

7. **Ensuring that the design, development, and use** of CCTV infrastructure, and all other smart city infrastructures, **are subject to a transparent, open, and public debate** even before the procurement stage.

8. **Ensuring the transparency and public oversight of procurement processes** for the acquisition, development, and deployment of smart city infrastructures including CCTVs and biometric technologies.

9. **Repealing laws that restrict access to information**, like the Official Secrets Act (1923), adopting a right to information law, and ensuring access to information in accordance with international human rights

standards. Information about existing technology procurement should be proactively made available to the public, as well as information about the extent of deployment, use, and impact of technologies like CCTV.

Given the current status quo, we make the following recommendations.

To the military junta in Myanmar

1. First and foremost, restore democracy and rule of law.

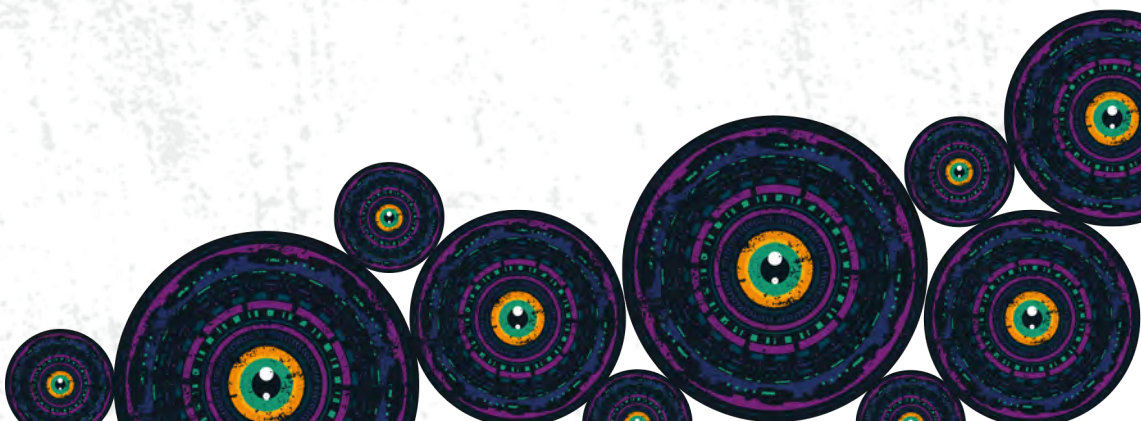
2. Immediately stop the purchase, development, and use of technologies that impact human rights, in particular emotion recognition technologies and other technologies described in this report.

To the private sector

1. Refrain from selling smart city infrastructures to authoritarian dictatorships or deploying such technology on their behalf.

2. Design, develop, and use smart city infrastructures including CCTV and biometric technologies in accordance with the UN's Guiding Principles on Business and Human Rights.

3. Perform and publish data protection impact assessments, human rights impact assessments, and risk assessment reports, and establish and adequately communicate procedures to mitigate risk and protect individuals' human rights and provide effective remedies when breaches occur.



Endnotes

[1] Smart cities are usually made up of a mix of technical infrastructure like public Wi-Fi, surveillance equipment like cameras and sensors, smart identification technologies, etc.

[2] S. Dirks and M. Keeling, 'A vision of smarter cities', *IBM Institute for Business Value*, December 2009, https://www.ibm.com/downloads/cas/2JYLM4ZA

[3] The Association of Southeast Asian Nations, 'ASEAN Smart Cities Network', *ASEAN*, November 2018, https://asean.org/our-communities/asean-smart-cities-network/

[4] ARTICLE 19, 'Biometric technologies: Freedom of expression must be protected', 21 April 2021, https://www.article19.org/resources/biometric-technologies-expression-must-be-protected/; Privacy International, 'Smart Cities: Utopian Vision, Dystopian Reality', October 2017, https://privacyinternational.org/sites/default/files/2017-12/Smart%20Cities-Utopian%20Vision%2C%20Dystopian%20Reality.pdf; Amnesty International, 'Ban the Scan', https://banthescan.amnesty.org

[5] G. Joseph, 'Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte', *The Intercept,* 20 March 2019, https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

[6] M. Prasad and V. Marda, 'Interrogating "Smartness": A Case Study on the Caste and Gender Blind Spots of the Smart Sanitation Project in Pune, India', *Global Information Society Watch*, 2019, page 4 https://giswatch.org/node/6174

[7] E. Morozov and F. Bria, 'Rethinking the Smart City: Democratizing Urban Technology', *Rosa Luxemburg Stiftung*, 22 June 2018, https://rosalux.nyc/rethinking-the-smart-city/

[8] J. Woetzel et al., 'Smart cities: Digital solutions for a more livable future', *McKinsey Global Institute*, 5 June 2018, https://www.mckinsey.com/business-functions/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future; PricewaterhouseCoopers, 'Smart Cities', https://www.pwc.com/gx/en/industries/government-public-services/smart-cities.html

[9] M. Mg, 'Myanmar soldiers are monitoring and watching the protestors at the traffic control center in Yangon #HearTheVoiceOfMyanmar #WhatsHappeningInMyanmar', Twitter, 7 February 2021, https://twitter.com/moramg20/status/1358465960299032578

[10] ARTICLE 19, Open Net Association, and the International Commission of Jurists, 'Myanmar: Scrap Cyber Security Draft Law and Restore Full Internet Connectivity', 12 February 2021, https://www.article19.org/resources/myanmar-scrap-cyber-security-draft-law-and-restore-full-internet-connectivity/

[11] V. Marda and S. Narayan, 'Data in New Delhi's Predictive Policing System', *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 2020, https://dl.acm.org/doi/abs/10.1145/3351095.3372865; K. Lum and W. Isaac, 'To Predict and Serve?' *Significance* 13 (2016): 14–19, https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x

[12] P.W. Kyaw, 'Mandalay receives Smart City Award', *Myanmar Times*, 2 September 2019, https://www.mmtimes.com/news/mandalay-receives-smart-city-award.html

[13] N. Lwin, 'Amid Int'l Espionage Concerns, Mandalay to Embrace Huawei for "Safe City" Project', *The Irrawaddy*, 19 June 2019, https://www.irrawaddy.com/opinion/analysis/amid-intl-espionage-concerns-mandalay-embrace-huawei-safe-city-project.html

[14] See a similar argument made in the African context by A. Williams, 'Some Myths Versus Realities of Africa-China Tech Narratives', *AI Now*, 28 May 2021, https://medium.com/@AINowInstitute/some-myths-versus-realities-of-africa-china-tech-narratives-75c97f43bf8a

[15] Reuters, 'Timeline: Events in troubled Myanmar since Suu Kyi's NLD party came to power', 31 January 2021, https://www.reuters.com/article/us-myanmar-politics-timeline/timeline-events-in-troubled-myanmar-since-suu-kyis-nld-party-came-to-power-idUSKBN2A112I

[16] S. Naing, 'Royal capital to "smart city": Myanmar's Mandalay gets high-tech makeover, sparks "spy" fears', *Reuters*, 3 August 2019, https://www.reuters.com/article/us-myanmar-mandalay-feature-idUKKCN1UU04Q

[17] N. Lwin, 'Mandalay chases dream of becoming Myanmar's first smart city', *The Irrawaddy*, November 28 2018, https://www.irrawaddy.com/features/mandalay-chases-dream-becoming-myanmars-first-smart-city.html

[18] Naing, 'Royal capital to "smart city"'.

[19] N. Lwin, 'Myanmar's Second Biggest City Receives Smart City Award 2019', *The Irrawaddy*, 29 August 2019, https://www.irrawaddy.com/news/burma/myanmars-second-biggest-city-receives-smart-city-award-2019.html

[20] N. Lwin, 'Making Myanmar's Last Royal Capital an ASEAN "Smart City"', *The Irrawaddy*, 23 November 2018, https://www.irrawaddy.com/in-person/making-myanmars-last-royal-capital-asean-smart-city.html

[21] Dr Ye Lwin was a member of the NLD government and the Mayor of Mandalay city. He was also the chair of MCDC as the key person behind the realisation of Mandalay's smart cities improvement. He was detained by the military on 10 February 2021, after resigning from his position following the coup. He was charged with sedition under Section 505(b) of the Penal Code, and his appeal against this decision was rejected in January 2022. https://www.irrawaddy.com/news/burma/myanmars-military-regime-brings-charges-incitement-ousted-nld-ministers.html;

https://www.irrawaddy.com/news/burma/myanmar-junta-sentences-ousted-nld-chief-minister-to-four-years-in-prison.html';
https://www.irrawaddy.com/news/burma/junta-court-rejects-appeal-for-myanmars-ousted-ruling-party-vice-chair.html

[22] The Association of Southeast Asian Nations, 'ASEAN Smart Cities Network Smart City Action Plans', 8 July 2018, https://asean.org/wp-content/uploads/2019/02/ASCN-Consolidated-SCAPs.pdf

[23] Lwin, 'Mandalay chases dream'.

[24] Naing, 'Royal capital to "smart city"'.

[25] T. Hlaing, 'Yangon to Put Up More CCTV Cameras in High-Crime Neighborhoods', *The Irrawaddy*, 7 June 2019, https://www.irrawaddy.com/news/yangon-put-cctv-cameras-high-crime-neighborhoods.html

[26] M.K. Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'], *Mratt's Channel*, 20 June 2021, https://mrattkthu.com/blogs/companies-which-help-sac-to-arrest-people. For a rough English translation: https://mrattkthu-com.translate.goog/blogs/companies-which-help-sac-to-arrest-people?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

[27] M. Thura, 'Nay Pyi Taw authorities activate 335 cameras able to detect faces', 23 December 2020, https://www.mmtimes.com/news/nay-pyi-taw-authorities-activate-335-cameras-able-detect-faces.html

[28] Assistance Association for Political Prisoners, 'Daily Briefing in Relation to the Military Coup', 30 September 2021, https://aappb.org/?p=17934

[29] Delta News Agency, 'မော် တော် ယာဉ်နံပါတ်ပြားတွေကို အပြောင်းအလဲလုပ်မယ်' ['Vehicle licence plates will be changed'], Facebook, https://www.facebook.com/662575584120143/posts/1418808451830182/?d=n

[30] R. Chandran, '"Fears of 'digital dictatorship" as Myanmar deploys AI', *Reuters*, 18 March 2021, https://www.reuters.com/world/china/fears-digital-dictatorship-myanmar-deploys-ai-2021-03-18/

[31] Human Rights Watch, 'Myanmar: Facial recognition system threatens human rights', 12 March 2021, https://www.hrw.org/node/378187/printable/print

[32] Mg, 'Myanmar soldiers'.

[33] ARTICLE 19, Open Net Association, and the International Commission of Jurists, 'Myanmar: Scrap Cyber Security Draft Law'.

[34] Eleven Media Group, 'Mandalay Mayor detained again', 9 February 2021, https://elevenmyanmar.com/news/mandalay-mayor-detained-again

[35] Myanmar Times, 'မန္တလေးမြို့တော်ဝန်အဖြစ်တာဝန်ပေးအပ်ခံရသူ ဦးကျော်ဆန်း တာဝန်စတင်ထမ်းဆောင်' ['U Kyaw San, the new mayor of Mandalay, takes office'], 11 February 2021, https://myanmar.mmtimes.com/news/151180.html
[36] Myanmar Now, 'မန္တလေးကို စောင့်ကြည့်မည့် ဟွာဝေးကင်မရာများ စစ်ကောင်စီကို အပ်နှံ' ['Huawei cameras to monitor Mandalay handed over to military council'], 19 June 2021, https://www.myanmar-now.org/mm/news/7162

[37] M.P. Phyo, 'Huawei to Supply Mandalay's "Safe City" Project with Cameras, Security Equipment', *The Irrawaddy*, 9 May 2019, https://www.irrawaddy.com/news/burma/huawei-supply-mandalays-safe-city-project-cameras-security-equipment.html

[38] CCTV Cameras Myanmar, 'Mandalay, Myanmar – Police Command Center', Facebook, 7 December 2015, https://www.facebook.com/CCTV.Cameras.Myanmar/posts/461288577405393/

[39] For more context on special departments within the Myanmar Police Force, see https://en.wikipedia.org/wiki/Myanmar_Police_Force

[40] R. Chandran, 'Fears of "digital dictatorship" as Myanmar deploys AI', Thomson Reuters Foundation, 18 March 2021, https://news.trust.org/item/20210318130045-zsgja/

[41] C. Norris, M. McCahill, and D. Wood, 'The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space'. *Surveillance & Society* 2, no. 2 (2004): 110–135.

[42] Forbes India, 'Delhi, Chennai among most surveilled in the world, ahead of Chinese cities', 25 August 2021, https://www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1

[43] Norris, et al., 'The growth of CCTV'.

[44] J. Rosen, 'A watchful state', *New York Times*, 7 October 2001, https://www.nytimes.com/2001/10/07/magazine/a-watchful-state.html; A. Linn, 'Post 9/11, surveillance cameras everywhere', NBC, 23 August 2011, https://www.nbcnews.com/id/wbna44163852

[45] F. Adams-O'Brien, 'Is there Empirical Evidence that Surveillance Cameras Reduce Crime?', *MTAS Research and Information Center*, September 2016, https://www.mtas.tennessee.edu/knowledgebase/there-empirical-evidence-surveillance-cameras-reduce-crime

[46] R.V. Liedka, A.J. Meehan, and T.W. Lauer, 'CCTV and campus crime: Challenging a technological "fix"', *Criminal Justice Policy Review* 30, no. 2 (2019): 316–338.

[47] M. Gill, J. Bryan, and J. Allen, 'Public Perceptions of CCTV in Residential Areas: "It Is Not As Good As We Thought It Would Be"', *International Criminal Justice Review* 17, no. 4 (2007): 304–324.

[48] A. Rathi and A. Tandon, 'Capturing Gender and Class Inequities: The CCTVisation of Delhi', *Development Informatics Working Paper* 81, (2019), https://www.gdi.manchester.ac.uk/research/publications/di/di-wp81/; A.M. Alkazi, 'Gated Communities in Gurgaon: Caste and Class on the Urban Frontier' (2015), *Senior Projects Spring 2015*, https://digitalcommons.bard.edu/senproj_s2015/114; Amnesty International, Internet Freedom Foundation and ARTICLE 19, 'Ban the Scan: Hyderabad', https://banthescan.amnesty.org/hyderabad/

[49] Human Rights Watch, 'Vote to Nowhere: The May 2008 Constitutional Referendum in Burma', 30 April 2008, https://www.hrw.org/report/2008/04/30/vote-nowhere/may-2008-constitutional-referendum-burma

[50] Free Expression Myanmar, Article 354 and 365 of the Constitution, https://freeexpressionmyanmar.org/constitution/

[51] L. Lakhdhir, 'The Criminalization of Peaceful Expression in Burma', Human Rights Watch, 30 June 2016, https://www.hrw.org/report/2016/06/30/they-can-arrest-you-any-time/criminalization-peaceful-expression-burma

[52] A. Abrahamiyan, 'Article 66(d): A menace to Myanmar's democracy', *The Interpreter*, 1 August 2017, https://www.lowyinstitute.org/the-interpreter/article-66d-menace-myanmar-s-democracy; Human Rights Watch, 'Burma: Letter on Section 66 (d) of the Telecommunications Law', 10 May 2017, https://www.hrw.org/news/2017/05/10/burma-letter-section-66d-telecommunications-law

[53] Free Expression Myanmar, https://freeexpressionmyanmar.org/right-to-information-bill/

[54] Myanmar Centre for Responsible Business, 'Policy brief: A data protection law that protects privacy: Issues for Myanmar', https://www.myanmar-responsiblebusiness.org/pdf/2019-Policy-Brief-Data-Protection_en.pdf

[55] Myanmar Centre for Responsible Business, 'MCRB provides initial comments to government on the draft cybersecurity framework, and discusses cybersecurity with MPs', 4 February 2019, https://www.myanmar-responsiblebusiness.org/news/draft-cybersecurity-framework.html

[56] P.P. Kyaw, 'The Rise of Online Censorship and Surveillance and Myanmar: A Quantitative and Qualitative Study', *Open Technology Fund*, November 2020, https://public.opentech.fund/documents/The_Rise_of_Online_Censorship_and_Surveillance_in_Myanmar.pdf

[57] Human Rights Watch, 'Myanmar: Post-Coup Legal Changes Erode Human Rights', 2 March 2021, https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights#

[58] P, 'မန္တလေးတွင် စောင့်ကြည့်ကင်မရာများတပ်ဆင်ရန် တရုတ် Huawei ကုမ္ပဏီနှင့် စာချုပ်ချုပ်ဆို' ['Signs contract with Chinese company Huawei to install surveillance cameras in Mandalay'], Myanmar Now, 11 December 2020, https://www.myanmar-now.org/mm/news/5196

[59] Phyo, 'Huawei to Supply Mandalay'.

[60] Lwin, 'Myanmar's Second Biggest City'.

[61] Naing, 'Royal capital to "smart city"'.

[62] Lwin, 'Amid Int'l Espionage Concerns'.

[63] S.C. Greitens, 'Dealing with demand for China's Global Surveillance Exports', *Brookings Institution*, April 2020, https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/. See also S.C.Greitens, Twitter post, 16 March 2021, 7:02am, https://twitter.com/sheenagreitens/status/1371635574617030661

[64] Lwin, 'Amid Int'l Espionage Concerns'.

[65] ISP China Desk, 'တရုတ် ဒစ်ဂျစ်တယ် ပိုးလမ်းမစီမံကိန်းနှင့် မြန်မာနိုင်ငံ' ['China Digital Silk Road Project and Myanmar'], 9 July 2021, https://ispmyanmarchinadesk.com/special_issue/digital-silk-road-of-china/

[66] Lwin, 'Amid Int'l Espionage Concerns'.

[67] M.P. Phyo, 'CCTV Contract with Huawei Will Guard Against Spying: Mandalay Chief Minister', *The Irrawaddy*, 18 July 2019, https://www.irrawaddy.com/news/burma/cctv-contract-huawei-will-guard-spying-mandalay-chief-minister.html

[68] Sandhi Governance Institute, 'Public–Private Partnership Monitoring in Myanmar: The New Yangon City Project', March 2020, https://sandhimyanmar.org/wp-content/uploads/2020/06/PPP-Monitoring-Report-Q3-The-New-Yangon-City-Project.pdf

[69] M. Moe, 'Myanmar Capital to Spend US$2.7 Million on CCTV Boost', *The Irrawaddy*, 23 January 2020, https://www.irrawaddy.com/news/burma/myanmar-capital-spend-us2-7-billion-cctv-boost.html

[70] N.H Lin and M. Min, 'Hundreds of Huawei CCTV cameras with facial recognition go live in Naypyidaw', Myanmar Now, 15 December 2020, https://www.myanmar-now.org/en/news/hundreds-of-huawei-cctv-cameras-with-facial-recognition-go-live-in-Naypyidaw

[71] Thu, 'စစ်ကောင်စီကို နည်းပညာ ဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[72] Lin and Min, 'Hundreds of Huawei CCTV cameras'.

[73] S.M. Mon, 'CCTV road traffic centre officially launched in Yangon', *Frontier Myanmar*, 16 May 2017, https://www.frontiermyanmar.net/en/cctv-road-traffic-centre-officially-launched-in-yangon/

[74] ISP China Desk, 'တရုတ် ဒစ်ဂျစ်တယ် ပိုးလမ်းမစီမံကိန်းနှင့် မြန်မာနိုင်ငံ' ['China Digital Silk Road Project and Myanmar'.

[75] Hlaing, 'Yangon to Put Up More CCTV Cameras'.

[76] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၂)' [Companies providing technical assistance to the military council | Part 2], *Mratt's Channel*, 30 June 2021, https://mrattkthu.com/blogs/companies-which-help-sac-to-arrest-people-part-2. For a rough English translation: https://mrattkthu-com.translate.goog/blogs/companies-which-help-sac-to-arrest-people-part-2?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

[77] Ibid.

[78] Ibid. Also see M.K. Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည် ကုမ္ပဏီများ | အပိုင်း (၂)' [Companies providing technical assistance to the military council | Part 3], *Mratt's Channel*, 30 June 2021 https://mrattkthu.com/blogs/companies-which-help-sac-to-arrest-people-part-3. For a rough English translation: https://mrattkthu-com.translate.goog/blogs/companies-which-help-sac-to-arrest-people-part-3?_x_trsl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

[79] Republic of the Union of Myanmar, Presidents' Office, Directive No. 1/2017, translated by Lincoln Legal Services (Myanmar) Limited, https://www.lincolnmyanmar.com/wp-content/uploads/2019/04/Tender-procedure-Presidents-Office-1-2017_NoCopy.pdf

[80] J. Owen, N. Myaing, and N.Y. Oo, 'The governance of public procurement in Myanmar's States and Regions', *The Asia Foundation*, November 2020, https://asiafoundation.org/wp-content/uploads/2020/12/The-Governance-of-Public-Procurement-in-Myanmars-States-and-Regions_EN.pdf

[81] Ibid.

[82] Republic of the Union of Myanmar, Presidents' Office, Directive No. 1/2017.

[83] Phyo, 'CCTV Contract with Huawei'.

[84] United Nations Office on Drugs and Crime, *United Nations Convention against Corruption* (2004), https://www.unodc.org/unodc/en/corruption/uncac.html

[85] Phyo, 'CCTV Contract with Huawei'.

[86] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[87] For example, see Information Technology and Cyber Security Department, Tender number ITCSD (3/2017), Ministry of Transport and Communications, 20 June 2017, https://web.archive.org/web/20200729101312/https://www.motc.gov.mm/sites/default/files/NCSC%20Tender%20Notice%202017-2018%20%2820-6-2017%29_0.pdf

[88] Based on observation of different documents: WikiLeaks, 'The Hackingteam Archives', https://wikileaks.org/hackingteam/emails/emailid/555579; P.P. Kyaw, 'The rise of online censorship and surveillance in Myanmar', November 2020, https://public.opentech.fund/documents/The_Rise_of_Online_Censorship_and_Surveillance_in_Myanmar.pdf; Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[89] Free Expression Myanmar, 'Right to Information Bill', 28 February 2017, https://freeexpressionmyanmar.org/right-to-information-bill/

[90] Distributed Denial of Secrets, 'Myanmar Financials', 20 February 2021, https://ddosecrets.com/wiki/Myanmar_Financials

[91] This table does not include amounts of each tender as this is not public knowledge. Who won the tender, and for what amount, is only announced by the respective department office to which the entities applied.

[92] Based on observation of different documents: WikiLeaks, 'The Hackingteam Archives'; Kyaw, 'The rise of online censorship and surveillance'; Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနသေည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[93] Myanmar National Portal, https://myanmar.gov.mm/tenders

[94] T. Walker, 'How Myanmar's Civil Disobedience Movement Is Pushing Back Against the Coup', *Voice of America*, 27 February 2021, https://www.voanews.com/a/east-asia-pacific_how-myanmars-civil-disobedience-movement-pushing-back-against-coup/6202637.html

[95] Myanmar Now, 'Military kills another protester in Mandalay and refuses to return the body to his family', 2 August 2021, https://www.myanmar-now.org/en/news/military-kills-another-protester-in-mandalay-and-refuses-to-return-the-body-to-his-family

[96] MeKong News, 'CCTV များဖြုတ်ပေးရန် ရန်ကုန်တော်လှန်ရေးလူငယ်များ အကူအညီတောင်းစာများဖြန့်ဝေ' ['Yangon Revolutionary Youth call for help to remove CCTV'], Facebook, 7 October 2021, https://www.facebook.com/363715110955099/posts/867362713923667/

[97] Lin and Min, 'Hundreds of Huawei CCTV cameras'; Moe, 'Myanmar Capital'; Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း(၂)' [Companies providing technical assistance to the military council | Part 3].

[98] Based on an analysis of media reports including Lwin, 'Amid Int'l Espionage Concerns'; *Myanmar Now*, 'မန္တလေးကို စောင့်ကြည့်မည့် ဟွာဝေးကင်မရာများ စစ်ကောင်စီကို အပ်နှံ' ['Huawei cameras to monitor Mandalay handed over to military council'].

[99] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[100] WikiLeaks, 'The Hackingteam Archives', https://wikileaks.org/hackingteam/emails/emailid/555579

[101] T. McLaughlin, 'Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists', *Washington Post*, 4 May 2019, https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html. See also L. Koeke et al., 'Mass Extraction', *Upturn*, 20 October 2020, https://www.upturn.org/work/mass-extraction/

[102] McLaughlin, 'Security-tech companies'.

[103] M.K. Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | နိဂုံး' [Companies providing technical assistance to the military council | Conclusion], *Mratt's Channe*l, 7 August 2021, https://mrattkthu.com/blogs/companies-which-help-sac-to-arrest-people-finale. For a rough English translation: https://mrattkthu-com.translate.goog/blogs/companies-which-help-sac-to-arrest-people-finale?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp.

[104] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၂)' [Companies providing technical assistance to the military council | Part 2].

[105] This corroborates findings from Greiten's analysis of Chinese surveillance technology exports around the world. See S.C. Greitens, 'Dealing with demand for China's Global Surveillance Exports', *Brookings Institution*, April 2020, https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/

[106] KBZ, 'KBZ Bank announces partnership with Huawei to offer greater financial access to all', 20 March 2018, https://www.kbzbank.com/wp-content/uploads/2019/05/KBZ-Huawei-partnership_ENG_20032018.pdf

[107] N. Lwin, 'Huawei Extends Cloud Services to Myanmar as Firms Go Digital', *The Irrawaddy*, 20 October 2020, https://www.irrawaddy.com/news/burma/huawei-extends-cloud-services-myanmar-firms-go-digital.html

[108] J. Devanesan, 'Info cyberwars – The dark side of tech in the Myanmar coup', *Tech Wire Asia*, 1 April 2021, https://techwireasia.com/2021/04/info-cyberwars-the-dark-side-of-tech-in-the-myanmar-coup/

[109] R. Chandran, 'Protesters fear they are being tracked by cameras armed with facial recognition technology', Thomson Reuters Foundation, 18 March 2021, https://news.trust.org/item/20210318130045-zsgja; Lin and Min, 'Hundreds of Huawei CCTV cameras'; Lwin, 'Amid Int'l Espionage Concerns'; Moe, 'Myanmar Capital', Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၂)' [Companies providing technical assistance to the military council | Part 3].

[110] Huawei, 'What is a Software-Defined Camera?', 9 April 2021, https://e.huawei.com/en/products/intelligent-vision/cameras/software-defined-camera

[111] Huawei, 'Huawei Intelligent Video & Data Analytics iCAN Evaluation Criterion White Paper', 3 January 2020, https://e.huawei.com/cn/material/enterprise/cc54add75d504a9eb9f2d9e407a6d722

[112] P. Parameswaran, 'What Will Myanmar's New Home Minister Mean for the Country's Security and Politics?', *The Diplomat*, 10 February 2020, https://thediplomat.com/2020/02/what-will-myanmars-new-home-minister-mean-for-the-countrys-security-and-politics/

[113] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[114] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), https://www.un.org/en/about-us/universal-declaration-of-human-rights

[115] UN General Assembly, *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) United Nations, Treaty Series, vol. 999, Article 21, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[116] UN Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

[117] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion*, UN Doc. A/HRC/38/35, 18 June –16 July 2018, page 5, para 10, https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F35&Language=E&DeviceType=Desktop

[118] ARTICLE 19, 'When Bodies Become Data', April 2021, https://www.article19.org/wp-content uploads/2021/05/Biometric-Report-P3-min.pdf

[119] See Article 17 (1) of the ICCPR. Also see Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/27/37, 30 June 2014, para 23, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. See also Necessary & Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance', https://necessaryandproportionate.org/principles

[120] C. Burt, 'UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition', *Biometric Update*, 3 July 2018, https://www.biometricupdate.com/201807/un-privacy-rapporteur-criticizes-accuracy-and-proportionality-of-wales-police-use-of-facial-recognition

[121] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, David Kaye*, UN Doc. A/HRC/29/32, 22 May 2015, para 14–18, https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F29%2F32&Language=E&DeviceType=Desktop

[122] Ibid, para 12.

[123] A. Theinkha and R. Finney, 'Hundreds Protest Police Naming of Child Rape Victim in Myanmar', *Radio Free Asia*, 23 December 2019, https://www.rfa.org/english/news/myanmar/naming-12232019170954.html

[124] Lin and Min, 'Hundreds of Huawei CCTV cameras'.

[125] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/3, para 21, 22, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

[126] ARTICLE 19, 'When Bodies Become Data'.

[127] London Policing Ethics Panel, *Final Report on Live Facial Recognition*, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

[128] UN Human Rights Council, *Rights to freedom of peaceful assembly and of association Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, UN Doc. A/HRC/41/41, 17 May 2019, para 57, https://undocs.org/Home Mobile?FinalSymbol=A%2FHRC%2F41%2F41&Language=E&DeviceType=Desktop&LangRequested=False

[129] For a discussion of the right to protest and what it entails for states, see ARTICLE 19, 'The Right to Protest: Principles on the protection of human rights in protests', 2016, https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf

[130] E. Selinger and A.F. Cahn, 'Did You Protest Recently? Your Face Might Be in a Database', *The Guardian*, 17 July 2020, https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database; The Wire, 'Delhi Police Is Now Using Facial Recognition Software to Screen "Habitual Protestors"', 29 December 2019, https://thewire.in/government/delhi-police-is-now-using-facial-recogni-tion-software-to-screen-habitual-protestors

[131] Human Rights Watch, 'Myanmar: Facial recognition system threatens rights'.

[132] MeKong News, 'CCTV များဖြုတ်ပေးရန် ရန်ကုန်တော်လှန်ရေးလူငယ်များ အကူအညီတောင်းစာများဖြန့်ဝေ' ['Yangon Revolutionary Youth call for help to remove CCTV'.

[133] Thu, 'စစ်ကောင်စီကို နည်းပညာဖြင့် အကူအညီပေးနေသည့် ကုမ္ပဏီများ | အပိုင်း (၁)' ['Companies providing technical assistance to the military council | Part 1'].

[134] For more information on this right, see ARTICLE 19, 'International Standards: Right to Information', https://www.article19.org/resources/international-standards-right-information/

[135] ARTICLE 19, 'Global: Exercise your right to information', 28 September 2021, https://www.article19.org/resources/global-exercise-your-right-to-information/

[136] Hlaing, 'Yangon to put up more CCTV cameras'.

[137] J. Carroll, 'The brutal reality transgender women face under Myanmar's 'darkness law'', *Mashable*, 19 March 2016, https://mashable.com/article/trans-women-myanmar

[138] UN News, 'UN human rights chief points to "textbook example of ethnic cleansing" in Myanmar', 11 September 2017, https://news.un.org/en/story/2017/09/564622-un-human-rights-chief-points-textbook-example-ethnic-cleansing-myanmar

[139] ARTICLE 19, 'Update on Myanmar' in *Global Expression Report 2018/2019*, https://www.article19.org/reader/global-expression-report-2018-19/regional-overviews/asia-pacific-regional-overview/asia-pacific-countries-in-focus/update-on-myanmar/

[140] The Administrative Tribunal of Marseille, 27 February 2020, req. n. 1901249.

[141] UN-Habitat Myanmar, 'Consultation Workshop on Smart City Strategy for National Urban Policy in Myanmar', 23 October 2019, https://unhabitat.org.mm/news/consultation-workshop-on-smart-city-strategy-for-national-urban-policy-in-myanmar/

[142] ISP China Desk, 'တရုတ် ဒစ်ဂျစ်တယ် ပိုးလမ်းမစီမံကိန်းနှင့် မြန်မာနိုင်ငံ' ['China Digital Silk Road Project and Myanmar'.

"In Myanmar, CCTV cameras are being weaponised to silence dissent. While the narrative of 'safety' encourages the purchase of these technologies, it is the ambition of surveillance and control that currently sustains it. It is vital that civil society examines not only how this power is wielded, but how it impacts dissent, and concentrates power across the country."


ARTICLE19
www.article19.org