ECDHR

Cyber Surveillance in the United Arab Emirates: Updated Assessment

Table of Contents:

Introduction

Since the First Arab Spring in 2011, the government of the United Arab Emirates (UAE) has restricted freedom of expression and association, from in-person protests to online activism. In 2023, the UAE ranked 145th out of 180 countries in the World Press Freedom Index, which measures media freedom in the respective countries. The UAE's position has lowered by 7 places since the previous year and by 26 places since 2019, demonstrating an alarming trend towards complete media censorship by the government.

In the past decade, the UAE has notoriously used cyber surveillance to infringe on the privacy of internet users, specifically by gathering information on human rights activists to unlawfully persecute them. It is important to note that the UAE is a signatory of the Arab Charter on Human Rights, in which Article 26 states that everyone should have the "freedom of opinion and expression, as well as the right to seek, receive and impart information and ideas through any medium". Therefore, the UAE's use of cyber surveillance to restrict the freedom of opinion of people and persecute them for it, is antithetical to the Charter they are legally bound to respect.

The most noteworthy scheme was when the UAE employed former US National Security Agency and CIA employees at DarkMatter, an Emirati cyber-security firm, to hack into the phones of hundreds of human rights activists and political opponents in 2016 and 2017. The ex-employees were part of Project Raven, which the Emirati government used to hack phones and computers across the Middle East and Europe. The news of this cyberattack only came to light in January 2019, three years after the project was thought to have launched. Three former U.S. Intelligence Community employees, Ryan Adams, Marc Baier and Daniel Gericke, admitted their involvement on September 15 2021, resulting in them relinquishing their security clearance and paying $1.68 million in exchange for their criminal charges being dropped. DarkMatter has not to date been prosecuted, although Saudi activist Loujain AlHathloul, who had been targeted by the program, did unsuccessfully file a lawsuit against them.

In December 2019 the New York Times unveiled that the Emirati messaging app ToTok was being used as spyware for mass surveillance. This app allowed the government to misuse the information that millions of users voluntarily, yet unknowingly, gave by accepting the privacy terms when downloading the app. The result was that the government was able to access conversations, both via messages and calls, locations, and contacts of the users to spy on them.

In the past five years, there have been escalations in the use of cyber surveillance, along with stricter cyber laws, which have led to severe concerns about human rights violations and the safety of activists and political opponents. In January 2022, another inquiry was led by the New York Times to investigate the connection between Israel's cyber-intelligence firm NSO Group's Pegasus spyware, and the UAE. It was revealed that Israel had sold Pegasus to the UAE to

reinforce their diplomatic relations, resulting in the UAE using Pegasus to hack the phone of a civil rights activist. This demonstrates a pattern of misuse of cyber-surveillance technologies by the UAE.

The UAE fortified its relations with Israel through the Abraham Accords in 2020, leading them to have access to Israel's advanced spyware. This poses a potential threat for non-allies and human rights activists as the strengthened cyber surveillance, along with the stricter cyber laws, will likely lead to forced censorship and increased unlawful persecution. The lack of transparency and accountability of the Emirati government regarding their use of cyber surveillance is a significant threat to human rights in the UAE and must continue to be addressed.

Cybercrime Laws in the UAE

Cybercrime laws play an important role in the infringement of the human rights of internet users. Online activity is heavily monitored in the UAE, and therefore the addition of strict cyber laws limits what people can legally post, which means that users must censor themselves if they wish to avoid being persecuted. On 20 September 2021, the Federal Decree-Law No. (34) of 2021 On Countering Rumors and Cybercrimes was enacted, further limiting the freedom of speech in the UAE. Article 1 of the legislation provides a vague definition of illegal content, which includes anything that "would decrease the public's confidence in any of the government authorities". This definition means that any online speech that criticises the government is deemed illegal, which would target many human rights activists and government opponents.

The most significant addition to the 2012 Cybercrime Law was that sharing false information, referred to as "rumours" in the legislation, via social media now carries a penalty of up to five years in prison and a fine of up to five hundred thousand dirhams (€128,000). Furthermore, Article 20 provides a sentence of up to life in prison for any internet users who "advocate the overthrow, change, or usurpation of the system of governance in the state, or obstruct provisions of the constitution or existing law, or oppose the fundamental principles on which the system of governance is based." This law allows the UAE authorities to imprison people for speaking out against the repressive government. As a result, the combination of strict cybercrime laws and excessive use of cyber surveillance threatens the human rights of internet users in the UAE by decreasing their freedom of speech.

The 2022 UAE Media Strategy aims to "manage the country's reputation" by delimiting what can be posted on traditional and digital media. Human Rights Watch has published that some journalists feel that their freedom of expression is being curtailed and that they must self-censor. This demonstrates a further trend towards more repressive policies which the UAE government is using to control the media and its reputation, at the expense of the freedom of its citizens.

Universal Periodic Review: Fourth Cycle Recommendation on Cyber Surveillance

On May 8 2024, the UAE underwent consideration for its fourth cycle of the Universal Periodic Review (UPR). The 2023 Working Group report included many recommendations regarding the right, or lack thereof, to freedom of expression, while only four targeted the UAE's cybercrime laws and cyber surveillance. Since the last UPR, the UAE has continued to infringe on the rights of the individuals in the country by violating their privacy through state-sanctioned surveillance. In addition, the current recommendations on cyber surveillance and online freedom have all only been noted, except for one which was supported, emphasising the UAE's reluctance to make a change. This demonstrates a continued lack of commitment from the government.

Costa Rica recommended that the UAE terminate all cyber surveillance operations, prohibit the use of spyware, and amend its cybercrime laws. The United States of America (US) and Switzerland did not mention cyber surveillance, but both recommended that the UAE amend its cybercrime law to bring it in line with international law and include the right to online freedom of expression. Other countries, such as Argentina, Austria, Belgium, Canada, and Estonia, all made recommendations regarding media and online freedom, with specific reference to protecting human rights defenders and journalists.

Austria's recommendation to "take steps to ensure adequate protection of media freedom, and safety of journalists, media workers and human rights activists from all forms of violence, harassment or intimidation", was the only one supported. This begs the question of why this specific recommendation was supported rather than the other nine which were similar in content. The main difference with this one is that it focuses more on the protection of the people than on the protection of their rights to freedom of expression. It also does not give a standard or international framework; "adequate protection" for Austria is likely to be very different to the UAE's definition. As a result, the part of the recommendation that could be linked to media surveillance is very vague and thus easier to support as a repressive government. There is also no specific mention of needing to amend domestic law or stop cyber surveillance, meaning that the UAE could follow this recommendation and keep its current cyber surveillance practices.

Given there were 323 recommendations, 50% more than the previous review, a total of 10 recommendations on this issue from eight countries shows that although there is international concern, there is not enough targeted pressure on the government to make changes. Many of the recommendations touched on the issue of freedom of expression, but not on online freedom and cyber surveillance. The UPR could be a powerful tool but with references to the need for

improved media and internet freedom being mentioned since the first review cycle, more needs to be done to ensure that the recommendations come to fruition.

Surveillance: online and off

In the past five years, the UAE has routinely scored 0 out of 6 for the question "Does state surveillance of internet activities infringe on users' right to privacy?" indicating a high level of infringement. Many of the local news sites, which are owned and controlled by the state, exercise self-censorship to avoid persecution. This results in very biased and censored news sharing, often obscuring the realities of what occurs in the UAE from other countries. This is especially detrimental from a human rights perspective, given that the activists who advocate for the truth are censored and detained under the Cybercrime Law.

As of January 2023, the UAE only regulates optical surveillance devices, such as CCTV cameras, leaving computer tracking and facial recognition unregulated. As a result, the UAE state and firms can track computers and use facial recognition to find peaceful activists and arbitrarily arrest them without breaking any national laws. In addition, given that the government controls the telecom operators Etisalat and Du, the security services can monitor all communications on their networks and track who is saying what. As a result, the government can collect and analyse communication data from all over the country, making its people fear to speak freely which leads to self-censorship. The fact that the government can track people's phones is enough to make journalists scared to write the truth, demonstrating how much power the government has over people's actions. As a result, the government weaponises the fear instilled into its people to control internet and media usage.

Although the UAE has ratified the Arab Charter on Human Rights, which gives the right to privacy and freedom to its residents and citizens, the lack of specialised international regulations for cyber surveillance allows the UAE to continue its harmful practices without any accountability. This leaves human rights activists unprotected.

The COP28 climate summit, held in Dubai from November 30 to December 2013 2023, brought considerable concerns to many human rights organisations over the safety of its participants. This is because the excessive number of surveillance cameras present were owned by the company linked to ToTok; the app accused of being used as spyware for mass surveillance. With a track record of misusing personal data and illegally tracking communications, many were scared that the CCTV recordings were being used by the state to listen to conversations and track anyone who disagreed with the government. This created a tense environment where activists chose not to speak openly about their concerns and hid their ID badges while at the demonstrations. The government allowed protests at the summit under strict guidelines, but with the looming threat of being caught on camera and later found through data tracking technologies,

this permission was under false pretences. Given that this summit generally attracts many climate and human rights activists, the government was able to use the presence of added surveillance to silence them, without physically intervening. As a result, the government's scare tactics to curtail freedom of expression have once again proven successful.

The fear of cyber surveillance and the misuse of data and tracking systems has transcended to offline activities whereby people censor themselves at large public events in fear of being targeted by the government.

Pegasus Program Used to Target Human Rights Victims

In 2021, the Pegasus Project, an investigation led by The Guardian and 16 other global media outlets, revealed that the Israeli company NSO Group was selling hacking spyware called Pegasus to governments. This spyware can be covertly installed into phones and gives the attacker access to the device's messages, emails, media, microphone, camera, calls, and contacts. NSO claims that it only sold the software to governments for national security usage, however, the investigation revealed that journalists, human rights activists, and leaders around the world were selected as possible targets for surveillance by the government clients.

One of the governments in question was that of the UAE, which has been a client of NSO since 2015. The New York Times was able to concretely show that Israel sold Pegasus to UAE as a "truce" to re-establish the UAE-Israel security and defence relationship. As a result, Pegasus symbolises the strong diplomatic alliance between the UAE, a state notorious for its unlawful cyber surveillance, and Israel, a powerful player in cybersecurity. This means it is more than just spyware, it is also a political statement of power.

The leaked data analysed by the Project revealed that the government had selected over 10,000 phone numbers to use the spyware on, which is the highest number behind Mexico and Morocco. After the Pegasus Project investigation was released, NSO ended the Pegasus contract with the UAE. This was also influenced by the news of the ruling by England's High Court that Dubai's ruler Sheikh Mohammed bin Rashid al-Maktoum had ordered the phones of his ex-wife and her lawyers to be hacked during the custody battle over their children. This news was announced a year after the ruling took place in March 2020 due to reporting restrictions. The judge ruled that Sheikh Mohammed was using intimidation techniques, through the use of cyber surveillance, to win the case. Given that at the time his ex-wife was in the UK and using a British number, the UAE government used Pegasus to spy on a foreign territory where it has no jurisdiction.

Ahmed Mansoor is another victim of the UAE's malicious use of Pegasus. He started receiving suspicious texts on August 10 2016 and, given his prior experience with spyware, he forwarded the messages to Citizen Lab researchers. They were able to positively identify the malware as being the Pegasus spyware belonging to the NSO group. Although on this occasion Pegasus was

unsuccessful, the UAE continued to track his phone which directly led to his unlawful detention on the night of March 19 2017.

It is evident that this spyware, which was allegedly created for cyber surveillance under national security, was abused by the UAE to track people. The extent of the tracking is impossible to confirm, but what is certain is that over 10,000 people ran the risk of being tracked. The immense scale of these operations, spanning outside the UAE and into Europe, illustrates the power that the government holds. Whether or not NSO Group was in the know of the government's misuses does not change the fact that the UAE has not been held accountable for its unlawful surveillance.

DarkMatter: Project Raven

Project Raven started in 2009 when the UAE contracted Cyberpoint, an American cybersecurity firm, to train and support the UAE in improving its cybersecurity. At the end of 2015, Project Raven was taken over by the Emirati cybersecurity firm DarkMatter, along with the three former USIC employees who provided American espionage technology and information without authorisation from the U.S. government. As a result, the Raven team was unlawfully using technology, such as the spy tool Karma, to help the UAE government spy on people and organisations, including Americans. Between 2015 and 2019, the team hacked the phones of countless people and passed on the information to the government.

After Reuters exposed DarkMatter in 2019, the firm was reorganised to focus solely on defensive cyber activities. In 2021, DarkMatter's defensive activities against cyber-attacks were transferred to Digital14, while in 2022 the cyber surveillance and spyware activities were transferred to Cyber Protection X Holdings (CPX). Although DarkMatter does not exist in the same capacity anymore, the technologies and knowledge built over the years have been redistributed amongst other firms and thus the essence of it remains alive. As a result, the threat of the UAE using spyware and cyber surveillance on its citizens and abroad remains high.

Charges against the three former USIC employees

Marc Baier, Ryan Adams and Daniel Gericke were brought to court by the United States of America under conspiracy charges, which include violating the U.S. Export Control and Computer Fraud and Abuse Laws. In addition to being one of the few cases of former U.S. intelligence operatives being prosecuted for hacking, it was the first time the department used the violation of the International Traffic in Arms Regulations (ITAR) to charge a hacking case, demonstrating the severity of the acts committed.

On September 7 2021, the defendants officially admitted their crimes and entered a Deferred Prosecution Agreement with the United States Attorney's Office for the District of Columbia and the United States Department of Justice National Security Division. This Agreement absolved them of their criminal charges in three years, in exchange for them resigning from any position they held linked to the UAE and relinquishing any current and future U.S. government security clearance, which includes future employment restrictions. They also had to pay $1,685,000 in penalties, which could only be reimbursed with the agreement of the U.S. government. After this Agreement terminates on September 14 2024, they are free to continue working for the U.S. government and all previous restrictions are lifted.

This unique case has brought speculations about the leniency of the Agreement. ITAR violations would usually carry a criminal penalty of a maximum of $1,000,000 per violation and/or imprisonment of up to 20 years. Furthermore, the Conspiracy to Commit Access to Device Fraud and Computer Hacking Offences carries a penalty of up to five years in prison and up to $250,000. Given this, the fact that the highest individual penalty was $750,000 with no imprisonment demonstrates that the penalties for this case were lenient. The outcome of these criminal charges ended in a noncriminal penalty, despite there being a clear admission of guilt and intent. Although this case does set a precedent of hacking cases being charged with conspiracy to violate ITAR and the Arms Export Control Act, the lenient outcome lacks substantive accountability considering the charges.

Al-Hathloul v. DarkMatter Group

DarkMatter Group has been taken to court by one of its victims; Loujain Al-Hathloul. She is a Saudi women's rights activist who was hacked by the Raven team at the request of the UAE government. DarkMatter hacked her iPhone to read her communications and locate her whereabouts, which resulted in her being detained in May 2018 for allegedly breaking Saudi Arabia's counter-terrorism law. She was extradited to Saudi Arabia where she was later imprisoned, tortured, and subjected to a five-year travel ban. After global campaigns and advocacy work, she was released from prison in February 2021, although her travel ban which should have ended on September 13 2023, remains active.

In 2021, the non-profit digital rights organisation Electronic Frontier Foundation aided Al-Hathloul in filing a lawsuit in the Oregon U.S. District Court against DarkMatter, and the three former USIC employees, for illegally hacking her iPhone. The lawsuit stipulated that DarkMatter and the former employees violated the Computer Fraud and Abuse Act, as well as committing crimes against humanity under the Alien Tort Statute.

The Defendants, Dark Matter Group, argued that the Court had no jurisdiction over them and thus presented a Motion to Dismiss. On March 16 2024, the Court granted the Defendant's Motion to Dismiss with the possibility of Al-Hathloul to amend her case and prove that the Court has jurisdiction, although no updates have been published since. The judge decided that as the hacking of Al-Hathloul's phone occurred outside of the U.S., and as the spyware DarkMatter purchased from U.S. companies was altered before it was used to hack her phone, the U.S. Court had no jurisdiction.

Given that DarkMatter is a UAE company and was set up by the government to spy on people, Al-Hathloul has no chance to bring it to Court in the UAE where there would be clear jurisdiction, leaving the U.S. as her only viable option. Even the judge of this Court acknowledged that if Al-Hathloul's claims were true, then the UAE would be a "hostile forum". As a result, if Al-Hathloul is unable to satisfactorily prove jurisdiction, DarkMatter may continue to not be made legally accountable for what it did.

As with the case against the three former USIC employees, there is a clear lack of accountability. All parties involved in Project Raven have not been criminally charged despite committing criminal acts. This sets a precedent for the UAE to continue its cyber surveillance and hacking without the fear of any legal repercussions.

The Future

The UAE is partnering with foreign entities to build cyber-security technologies and gain cyberspace sovereignty. This sovereignty entails pushing for national rather than international regulations, which could lead to no standardised monitoring of how cybersecurity technology is used in the UAE. Given the backdrop of spyware abuses from the government, this move towards sovereignty could be detrimental to the human rights of its residents. Without any international regulatory body for spyware and cyber surveillance, the UAE can continue to spy on its residents and use it to detain activists and political opponents unlawfully.

The Abrahams Accord poses a threat to the safety of the residents because it gives the UAE access to increasingly sophisticated cyber-surveillance technologies. This cooperation will directly facilitate the targeted surveillance of its residents. Hamad al-Shamsi, an Emirati activist who advocates against the Abrahams Accord and the UAE's strengthened relations with Israel, declared that this agreement has already increased repression in the UAE and will only continue to do so due to the government's lack of accountability. This alarming move towards an even more repressive government threatens the privacy and human rights of many in the UAE.

In addition to UAE's bilateral agreement, the UN Cybercrime Treaty has been negotiated by its member states since May 2021. Although it would be the first treaty to address cybercrimes, its implementation is highly contented. The biggest concern is that at the moment, with five of the six negotiation sessions completed, there are insufficient human rights safeguards in place. The repercussions of this would be that autocratic governments, such as the UAE, could use this treaty to criminalise freedom of speech online. With the UAE's proven lack of criminal consequences for its acts and the improved cyber-surveillance technologies, this treaty has the prospect of further undermining the human rights of online users. The future of cyber surveillance in the UAE must be taken seriously as it is a real threat to its residents and citizens, especially human rights defenders and journalists.

Concluding Remarks

The UAE has used cyber surveillance to violate the rights of activists and journalists for over a decade. It has done so by misusing foreign government's technology, namely Pegasus spyware and Karma, to track innocent people. Although the precise scale of these violations is unknown, the Pegasus programme alone could have been used on over 10,000 people.

Although DarkMatter is reportedly no longer in the field of cyber surveillance, its knowledge and programmes could still be in use in Digital14 and CPX. Furthermore, the ex-employees who entered the Deferred Agreement will, as of September 14 2024, be free to work for either the UAE or the US government. As a result, the threat of another scheme such as the Raven Project will remain alive for the foreseeable future.

The issue of cyber surveillance is far beyond simply the infringement on the rights to privacy of internet and phone users. Without an understanding of the wider human rights issues of censorship and arbitrary detentions, one cannot fully understand the full extent of the UAE's violations. The surveillance systems are used to build fear and censor people from speaking the truth about the violations occurring in the country. Therefore, even if an individual is not currently being tracked, the possibility of it happening is omnipresent, especially for activists and journalists. This leads to the government controlling them without any direct contact. In addition, it allows the authorities to arbitrarily detain innocent activists. Given the repressive legislation that incriminates activists for peacefully protesting, cyber surveillance has been used as a tool to find and silence the voices of those the government disagrees with.

With international organisations coming together to uncover the UAE's cyber-surveillance violations from years prior, there is no concrete way of knowing whether there are currently more cases that have gone undetected. As a result, the international community must continue to

monitor the situation and advocate for the rights of internet users and the online freedom of expression in the UAE.

Recommendations

Given the dire human rights violations caused by the UAE's cyber surveillance, the following recommendations should be taken into consideration:

1. An international regulatory body must be set up to monitor cyber surveillance globally to ensure an ethical standard is set so that it is not misused to spy on citizens.
2. The UAE's NHRI must advocate for increased transparency and accountability of the government's use of spyware on residents and citizens.
3. The other signatories of the Arab Charter on Human Rights must keep the UAE accountable for its transgressions and ensure it abides by the Charter.
4. Governments and companies globally must stop dealing with the UAE in the sector of cybersecurity to avoid buying spyware and sharing intel with the UAE.
5. The UAE's Cybersecurity Council must set up a detached and independent branch that monitors the use of spyware on residents, including by government and UAE companies.
6. Human rights organisations must work together to advocate for the freedom of journalists and human rights activists unlawfully detained for peacefully voicing their concerns online.
7. The UAE government must ensure that its cybercrime laws are in line with international and regional standards on freedom of expression and media freedom.
8. In regards to the UN Cybercrime Treaty, the member states must remain committed to strong human rights standards. It is imperative that safeguards are put in place to ensure that repressive governments cannot take advantage of this treaty.