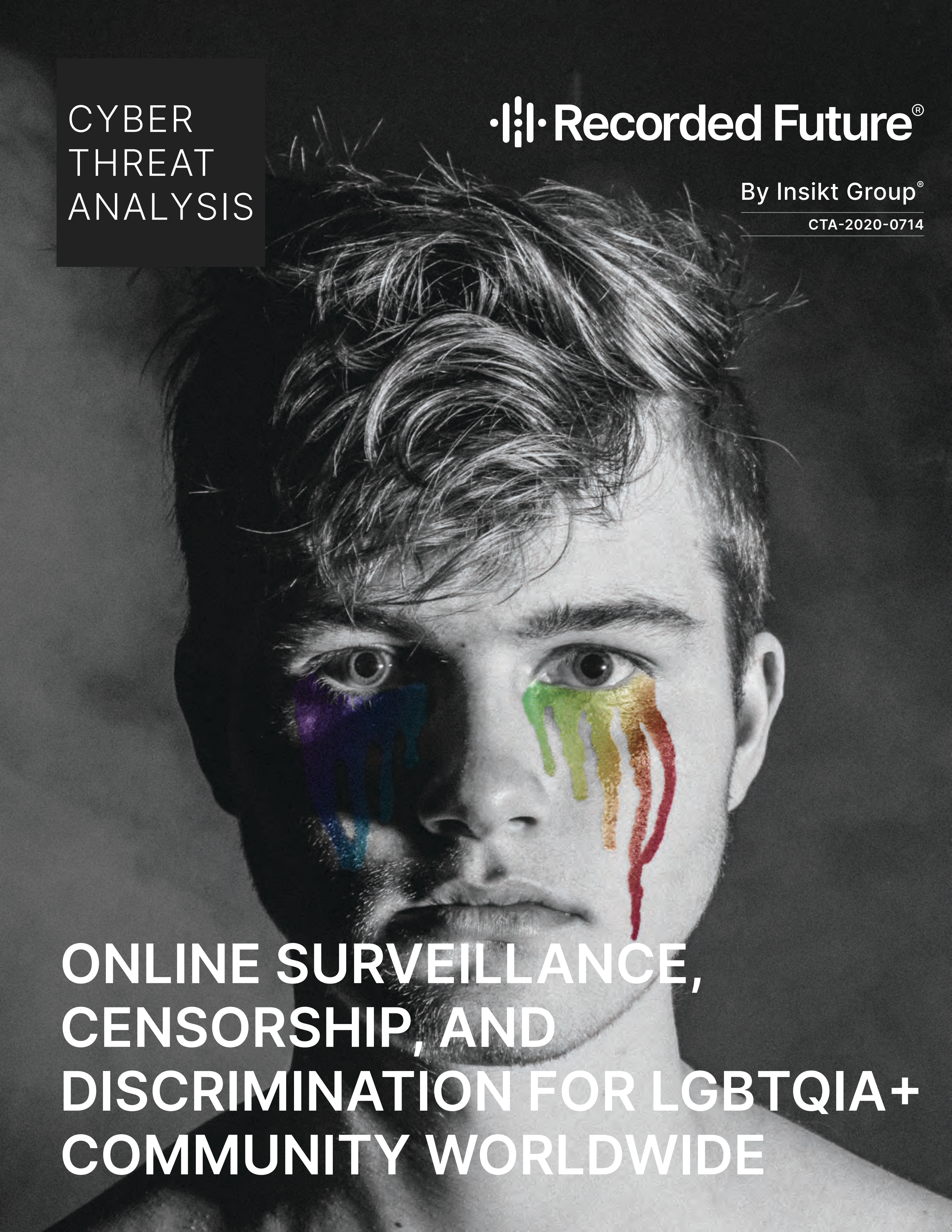


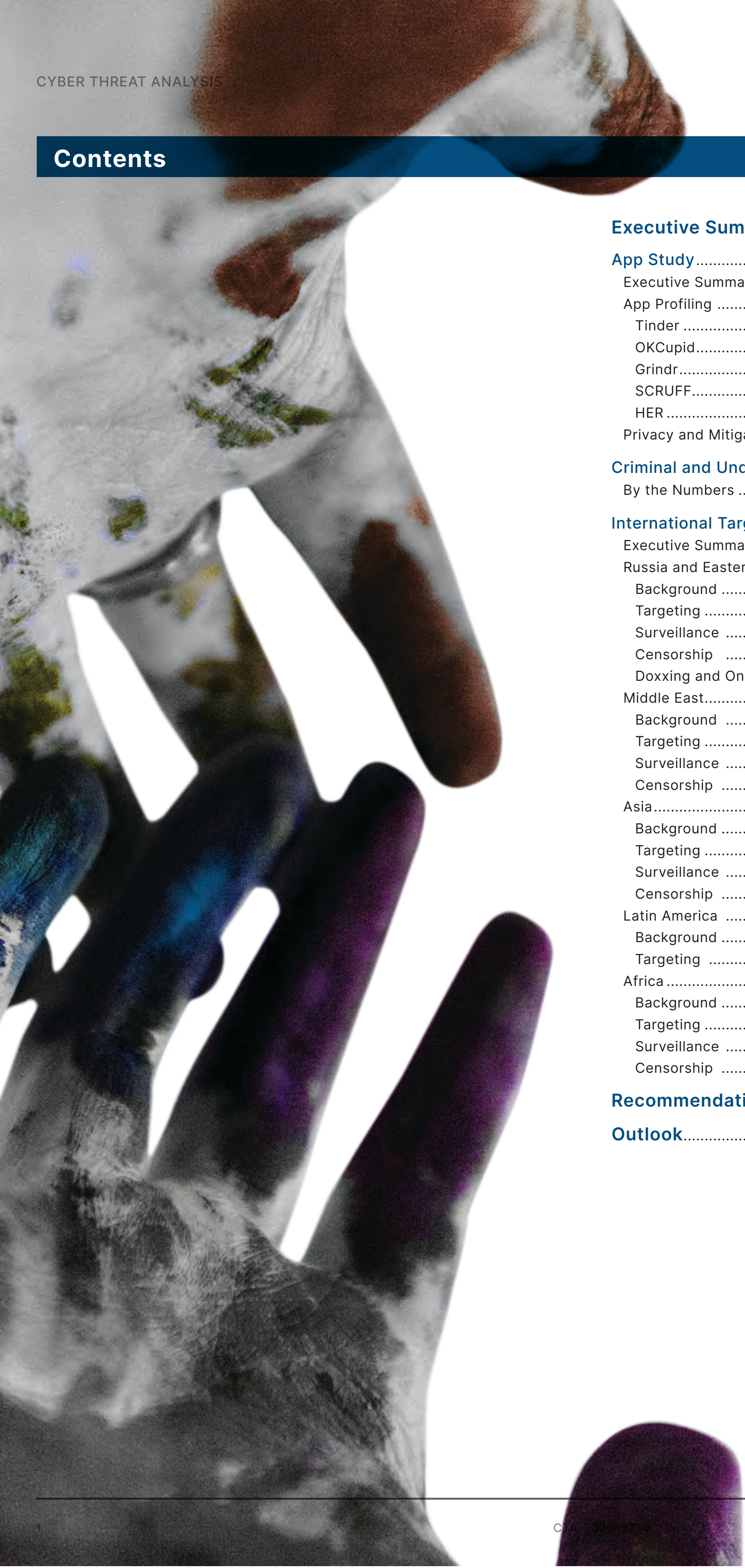
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-0714

ONLINE SURVEILLANCE, CENSORSHIP, AND DISCRIMINATION FOR LGBTQIA+ COMMUNITY WORLDWIDE



Contents

Executive Summary 2
App Study 3
Executive Summary 3
App Profiling 3
Tinder 3
OKCupid 4
Grindr 4
SCRUFF 4
HER 5
Privacy and Mitigation 5
Criminal and Underground Threat Activity 6
By the Numbers 6
International Targeting, Surveillance, and Censorship 7
Executive Summary 7
Russia and Eastern Europe 8
Background 8
Targeting 9
Surveillance 9
Censorship 9
Doxxing and Online Stalking 10
Middle East 10
Background 10
Targeting 11
Surveillance 11
Censorship 12
Asia 12
Background 12
Targeting 12
Surveillance 13
Censorship 13
Latin America 14
Background 14
Targeting 15
Africa 15
Background 15
Targeting 16
Surveillance 17
Censorship 18
Recommendations 19
Outlook 19

Executive Summary

During Pride Month, Recorded Future's Insikt Group partnered with Out@RF, the LGBTQIA+ (Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, Asexual) Employee Resource Group at Recorded Future, to conduct research into a range of cyber threats facing the LGBTQIA+ community on an international scale. The aim of this research is to raise awareness and visibility, and to provide pragmatic recommendations to help equip the LGBTQIA+ community in combating the threats that they face around the globe.

Recorded Future investigated data security risks associated with multiple social and dating apps that are popular with the LGBTQIA+ community, and how those apps were being discussed on dark web and underground sources. We also conducted research into the international targeting, surveillance, and censorship of the LGBTQIA+ community across Russia and Eastern Europe, the Middle East, Asia, Latin America, and Africa.

We researched Tinder, OKCupid, Grindr, SCRUFF, and HER and identified known security risks associated with these platforms. SCRUFF is doing the most proactive work to secure the data of its users, including randomizing location data and issuing alerts when users travel to countries that criminalize homosexuality, cutting ties with ad- and location-data brokers, and establishing in-house ad and analytics operations to avoid third-party sharing. By contrast, OKCupid, Grindr, and Tinder have been found to collect user data — including users' exact location, sexual orientation, religious beliefs, political beliefs, drug use, and more — and share that data with at least 135 different third-party entities.

Recorded Future observed multiple instances of broadly defined cyberattacks (including targeted cyberattacks, censorship, and surveillance) targeting LGBTQIA+ communities and individuals in Russia and Eastern European nations. Surveillance and censorship was widespread across Russia and Eastern Europe with many nations passing restrictive legislative policies against open expression of LGBTQIA+ content online.

Members of the LGBTQIA+ community in the Middle East have been met with limited freedoms and protections against discrimination and endured online attacks, surveillance, and censorship. In many countries, governments have used domestic telecommunications companies to block pro-LGBTQIA+ apps and websites. Further, Recorded Future has found that law enforcement and, very likely, intelligence agencies have deployed the use entrapment to expose members of the LGBTQIA+ community for imprisonment and torture.

Similar activity was observed affecting LGBTQIA+ individuals in various Asian countries in the past five years, specifically Azerbaijan, China, Georgia, India, Indonesia, Malaysia, Myanmar, Pakistan, Singapore, South Korea, and Sri Lanka. Many of these attacks were instigated by the state for censorship or surveillance purposes, or by individual actors motivated by financial interests or social stigma.

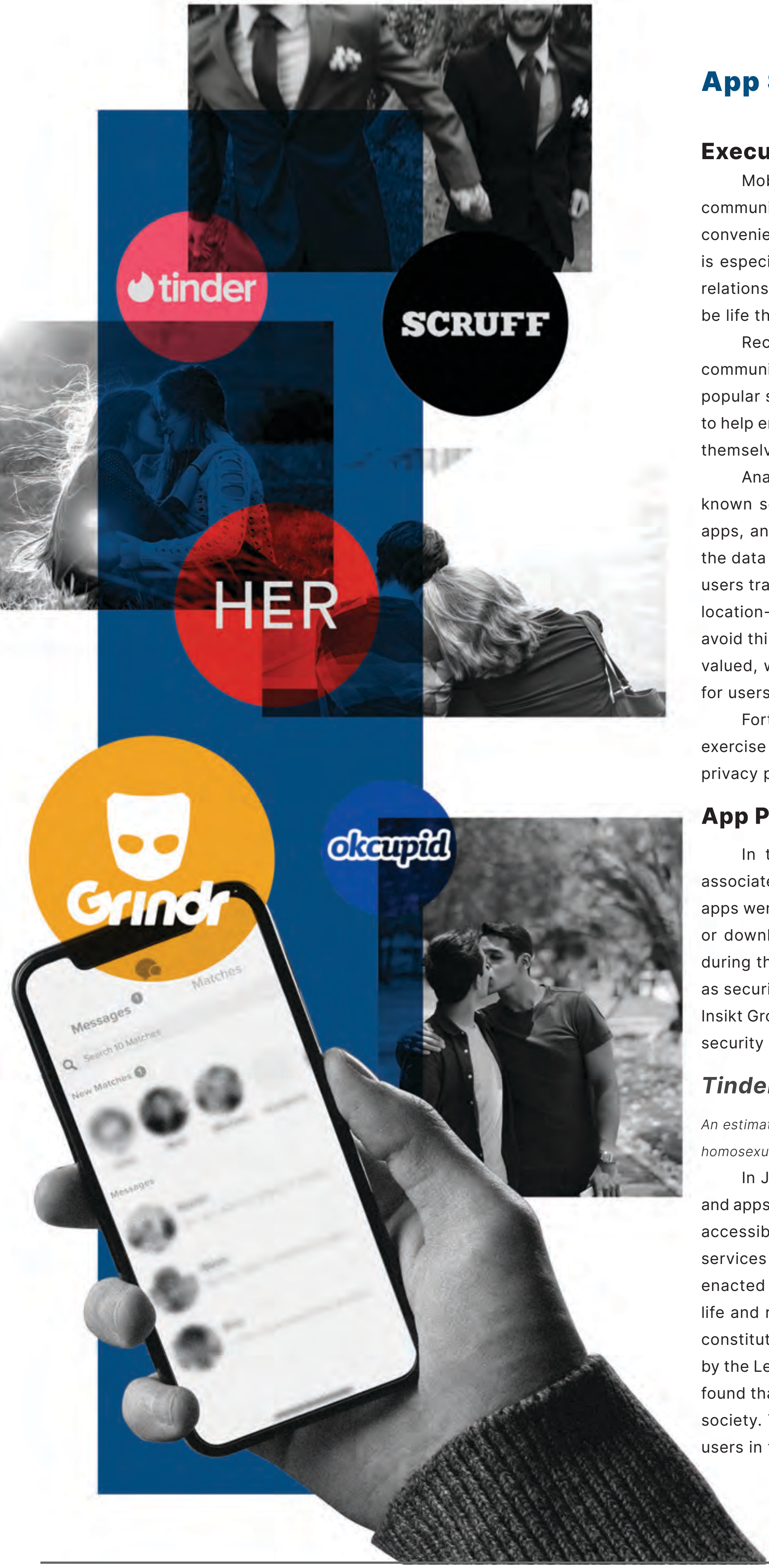
Over the past decade, Latin America has been a bright spot for LGBTQIA+ rights, and the region now leads the Global South in terms of legal protections for the community. However, violence against the LGBTQIA+ community, albeit not state-directed, is still a significant issue. The region's religious tradition and history of authoritarianism has kept much of the LGBTQIA+ community on the fringes of mainstream society, and many governments do not make a coherent effort to report or even respond to violence or other issues facing the community. The lingering social stigma towards the LGBTQIA+ community and the growing influence of evangelical Christian groups in Brazil and Central America pose the greatest threats to LGBTQIA+ rights in the region.

Across much of Africa, the LGBTQIA+ community is perceived as a threat to society that states are combating through organized crackdowns, surveillance, and censorship. In some instances, African governments are partnering with private sector surveillance organizations to target "high risk" groups, which includes the LGBTQIA+ community. Entrapment by law enforcement agencies and criminals is a common theme observed across Africa, with the outing of LGBTQIA+ individuals posing a significant threat due to strict anti-LGBTQIA+ legislation and socially conservative views among the public.

Looking ahead, further data exposures from social and dating apps popular with the LGBTQIA+ community, such as those that affected Grindr and Jack'd, are likely. These apps will almost certainly continue to share data with third parties and only user pressure, or a substantial fine for breaching data privacy laws, is likely to make these apps reconsider. Compromised account credentials and user data from social and dating apps will continue to be posted on dark web and underground sources. This offers an extortion opportunity for cybercriminals who could purchase leaked credentials to obtain intimate personal details and photos of individuals.

Nation-states will continue to target, surveil, and censor the LGBTQIA+ community for as long as they view the community as an external threat to security, society, or morality. Criminalizing the community will continue to encourage criminal acts against the community.

Users should exercise caution when using apps that use location data and learn more about the privacy policies of specific apps (Tinder, OKCupid, Grindr, SCRUFF, HER), paying particular attention to the apps that do not obfuscate geolocation data in countries with a poor stance on LGBTQIA+ rights. Users should also follow general best practices for cybersecurity, such as using multi-factor authentication and password managers like LastPass to manage long, unique passwords that are not reused across multiple accounts.



App Study

Executive Summary

Mobile device apps are an integral part of everyday life; they are used for communicating, sharing, and even finding love. While apps assist in making life convenient and interesting, they also collect sensitive data about their users. This is especially the case for some LGBTQIA+ users who live in regions where their relationships or identity are stigmatized or illegal. The exposure of their data can be life threatening.

Recorded Future's Insikt Group worked alongside Out@RF, the LGBTQIA+ community and allies within Recorded Future, to identify data security risks within popular social apps used by the LGBTQIA+ community. Recorded Future's goal is to help empower the LGBTQIA+ community with the knowledge to properly protect themselves and be aware of how their data is used and shared on social apps.

Analysts researched Tinder, OKCupid, Grindr, SCRUFF, and HER and identified known security risks associated with these platforms. Out of these five social apps, analysts believe that SCRUFF is doing the most proactive work to secure the data of its users, including randomizing location data and issuing alerts when users travel to countries that criminalize homosexuality, cutting ties with ad- and location-data brokers, and establishing in-house ad and analytics operations to avoid third-party sharing. These actions ensure its users are safe, protected, and valued, which is essential for vulnerable communities and potentially life saving for users.

Fortunately, online dating does not have to be a zero sum game. Users should exercise caution when using apps that use location data and learn more about the privacy policies of specific apps (Tinder, OKCupid, Grindr, SCRUFF, HER).

App Profiling

In this section, Insikt Group highlights security and privacy concerns associated with five popular social apps within the LGBTQIA+ community. The five apps were chosen based on their popularity, as assessed by the numbers of users or downloads: Grindr, Tinder, HER, OKCupid, and SCRUFF. Topics investigated during this research include how these apps collect and share user data, as well as security measures these companies are putting in place to protect their users. Insikt Group believes that of these five apps, SCRUFF appears to address its users security and privacy concerns most proactively.

Tinder

An estimated 50 million users worldwide (2020). Around 12% of male Tinder users identified as homosexual or bisexual, while only 0.01% of female profiles did (2016).

In June 2019, Russia's telecoms regulator added Tinder to a list of websites and apps that are forced to store user data, messages, and pictures on government-accessible Russian servers. This would allow law enforcement and intelligence services to use this data whenever requested. In 2013, the Russian government enacted a policy that criminalizes public and online expressions of LGBTQIA+ life and relationships. Later, in March 2020, President Vladimir Putin proposed a constitutional amendment banning gay marriage, and a recent survey conducted by the Levada Center, a nongovernmental research organization based in Moscow, found that one in five Russians wanted to "eliminate" gay and lesbian people from society. The ease of accessibility to this data from Tinder could be used against users in the LGBTQIA+ community to track and potentially punish individuals.

In July 2019, Tinder began rolling out new features in an attempt to protect users in the LGBTQIA+ community. First, based on geolocation of the user, Tinder would send notifications to inform readers of potential risks of using social apps for LGBTQIA+ people in almost 70 countries that have discriminatory laws. In addition, Tinder began to make the accounts of users in these countries private if their sexual orientation was considered illegal. While this is a step in the right direction to protect users, it also raises questions on where and how securely this data is being stored along with who has access to the data.

OKCupid

About 50 Million users as of 2019 (website and mobile app combined).

On January 14, 2020, the Norwegian Consumer Council published a report that found 10 Android apps collecting sensitive data — including users' exact location, sexual orientation, religious beliefs, political beliefs, drug use, and more — and sharing that data with at least 135 different third-party entities. Apps involved in this behavior that are also included in this list include OKCupid, Grindr, and Tinder. According to the Norwegian Consumer Council, this data harvesting appears to violate General Data Protection Regulation (GDPR), a regulation in the European Union's law on data protection and privacy. The results of the study were also alarming to Public Citizen in the United States, a consumer advocacy group that believes Congress should refer to the study's findings to pass a new law similar to GDPR.

When investigating OKCupid for the study, the Norwegian Consumer Council found that the app shares aforementioned details with an analytics company named Braze. According to Match Group, the company that owns OKCupid and Tinder, "all Match Group products obtain from these vendors strict contractual commitments that ensure confidentiality, security of users' personal information and strictly prohibit commercialization of this data." However, the Norwegian Consumer Council notes how privacy policies often do not provide comprehensive representations on how user data is being used, collected, or shared.

Grindr

30 million downloads as of June 2019.

Grindr has exposed its users' data in the past. In April 2018, researchers revealed that the social app was sharing sensitive information of users with third-party companies. This data included H.I.V. status, sexual tastes, and other intimate personal details. In August 2019, Pen Test Partners reported that Grindr, along with Romeo and Recon, were revealing its users' location data, putting users' physical security at risk. In January 2020, reports from the Norwegian Consumer Council claimed that Grindr was also transmitting user tracking codes along with the app's name to more than a dozen companies. In an investigation conducted by the New York Times, they found that the app shared precise user location with five companies. While it is common practice for apps to share user data with companies to perform certain tasks, this could be inherently dangerous for users, especially those in the LGBTQIA+ community.

If this data is shared with a third party, it is possible that the data could be shared further with organizations or governments with malicious intent. Not only do they have the location data of the user, but they know the sexual orientation of the user based solely on the purpose of the app.

Grindr also raised national security concerns according to a report from January 2020. In this report, John Demers, assistant attorney general for national security at the Department of Justice, expressed concerns over the amount of data collected by social apps, especially those owned by Chinese organizations. Grindr falls under that category as it is owned by the Chinese gaming company Beijing Kunlun Tech. According to Demers, data collected by Chinese companies is at risk for exposure to the Chinese government. "Chinese law requires a Chinese company to share any information that it has with the Chinese government if it's asked for that information for national security reasons."

SCRUFF

As of 2019, there are more than 15 million gay, bi, trans, and queer users who identify as men worldwide, with SCRUFF downloads taking place in 180 countries and six continents.

As of 2019, SCRUFF, an international social app for gay, bisexual, and transgender men, had more than 15 million users, with downloads throughout 180 countries and six continents. In July 2019, SCRUFF acquired the dating app Jack'd, after Jack'd agreed to pay $240,000 USD in a settlement with the New York Attorney General's office for exposing nude photos of approximately 2,000 New York users via an unsecured Amazon cloud server. Additionally, a second vulnerability in Jack'd exposed users' location data, device ID, operating system version, last login date, and hashed passwords.

On SCRUFF's support website, they have a section titled "LOCATION SECURITY & PRIVACY: AN INSIDE LOOK," in which they discuss concerns surrounding the privacy and security of location-based apps. In this section, SCRUFF alludes to some news headlines regarding the exposure of user data for apps such as Tinder and Grindr. Using these events as examples, SCRUFF's CEO, Eric Silverberg, details how SCRUFF addresses concerns regarding the security and privacy of its users' location data. Silverberg stated: "when a user elects to hide his distance on SCRUFF, we not only remove the information from his profile data, but we also randomize his location on our servers...we take density into account, so if [a user] live[s] in the city, [their] location will be randomized by a few blocks, but in the country it could be a few miles or more."

In addition to the measures SCRUFF takes to protect users' location data, it also engages in a partnership with the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA), a non-profit that publishes an annual report of gay and lesbian rights worldwide. Using this partnership, SCRUFF plans to implement a similar safety feature as Tinder that will alerts users when traveling to areas that have local laws that criminalize homosexual activity.

In April 2020, Silverberg interviewed with the news website Protocol about phone tracking and how location data is being used to study the spread of COVID-19. In the interview, Silverberg informed Protocol that in 2018, SCRUFF stopped doing business with third-party ad brokers and began using newly built in-house advertising and data analytics. In addition to ad brokers, SCRUFF is also committed to rejecting the sale of users' location data to location brokers. This decision is significant — as the world continues to address the ongoing COVID-19 pandemic, mobile carriers and app developers are deciding to share location data with authorities in an effort to help track and study the spread of the disease. However, Silverberg understands the importance of protecting the data of SCRUFF's users and the inherent risk in sharing user data with third parties whose practices SCRUFF knows little or nothing about. Silverberg states that SCRUFF's decision to not share user data is influenced by the privacy concerns of its users, especially when user identification could lead to physical harm or arrest.

HER

As of May 2020, HER has 4 million users in more than 50 countries.

HER, previously Dattch, claims to be the world's largest dating application for LGBTQIA+ women. HER also describes its services to include "a platform for dating, making friends, reading content, finding out about local events, or just chatting with the biggest community for queer people worldwide." The company, which was founded by and for lesbian and queer women, is headquartered in San Francisco, California and, according to a description of the application on the iTunes app store, has 4 million users.

The Terms of Service (ToS) for the application indicate that impersonation on the platform, data scraping, posting content in violation of law or the platforms rules, posting bulk messages or texts (spam), or efforts to "circumvent any technological measure implemented by HER or any of HER's providers or any other third party" are prohibited. Users have a right to cancel their service at any time; however, the platform indicates that, "if your Account is cancelled, we do not have any obligation to delete or return to you any of Your Content that you have posted to the Services." HER's ToS also indicate that they may "transfer our rights and obligations under these Terms to another organization — for example, this could include another member of our group of companies or someone who buys our business."

According to their Privacy Policy, HER collects personally identifiable information (PII) provided voluntarily by the user, as well as information obtained from third parties, communications with the company, survey data, sweepstakes or giveaway information, information provided to Facebook or other integrated social networking sites, technical data such a log files and cookies, mobile device use data, and location information.

HER indicates that they may use third-party analytics to determine how subscribers are using HER's services. HER's privacy policy indicates that it allows a user "the opportunity to connect automatically with your friend" via accessing Facebook contact data or contact information from a users mobile device, stating that, "with your permission, we will access your address book, call log and SMS log, and import your contacts' names, e-mail addresses, phone numbers, image, geographic location and Facebook IDs to facilitate automatic connection with your friends."

The privacy policy indicates that such data sharing can be "de-linked" and privacy sharing settings can be modified in some cases, but these changes must be made by the user via the "preferences" settings in the account. HER claims that PII data is collected to facilitate communication on the platform. While HER indicates that PII data is anonymized when used to perform data analytics, the company retains that information, which is transferable in the event the business ownership changes.

Privacy and Mitigation

Finding secure mobile apps in general is difficult, as noted by other security researchers. However, when it comes to queer social apps, Professor of Law at New York University Ari Waldman asserts that they may even be unsafe as a result of these security flaws. Instances of LGBTQIA+ individuals being targeted through social apps is not uncommon; extortion, catfishing, and revenge porn are common on queer dating platforms.

Some apps are taking strides to address privacy concerns of queer users. Hinge, for example, made a commitment to privacy by designing in automatic deletion of all communications the moment users delete their accounts. SCRUFF also makes it easy to flag offending accounts within the app and claims to respond to all complaints within 24 hours. Other apps, however, leave users to fend for themselves, as demonstrated by Grindr and the case of Matthew Herrick.

Geolocation features on some social apps have also posed significant privacy risks for queer users. Apps like SCRUFF, as previously mentioned, are using advanced measures to obscure users' locations should they choose to opt out of the feature. While apps like Tinder and HER also use geolocation features to match users within a dedicated radius, their location policies are less transparent.

While the temptation to delete social apps altogether might be appealing, for some, the digital risks are acceptable in their search for companionship. Users should exercise caution when using apps that use location data and find out more about specific apps privacy policies (Tinder, OKCupid, HER, SCRUFF, Grindr), especially when living in or visiting countries that persecute members of the LGBTQIA+ community.

Criminal and Underground Threat Activity

Mobile apps continue to become increasingly relevant to essential, everyday tasks, such as communicating with friends and family, tracking finances, and finding transportation. As apps percolate deeper into the personal lives of users, those users likewise share more of themselves with these apps (like personal information and location data), increasing their risk exposure. This is especially true for social apps, where personal profiles are the focus and can leave users susceptible to social engineering attacks. As a historically marginalized group, members of the LGBTQIA+ community have a particularly high risk of being targeted because of their identity or relationships.

We searched for threat activity targeting popular LGBTQIA+ social apps on dark web and underground sources over the past year. The following apps were chosen to be included based on research from the earlier App Profiling section: Grindr, Tinder, HER, OkCupid, SCRUFF, Growlr, Jack'd, Chappy, Hornet, Hinge, and Scissr.

Of the aforementioned social apps, Insikt Group believes that OkCupid is the most targeted by members of dark web and underground markets and forums, with Tinder also being heavily targeted. SCRUFF, Chappy, and Scissr were the least targeted, with no mentions across Recorded Future's dark web and underground sources. Across all of the chosen social apps, 77% of the targeted activity is listings for the sale of compromised account credentials and associated user data on dark web markets. Additionally, 6% of the targeted threat activity came from data dumps containing email addresses that use these apps' email domains — likely internal or employee accounts — including a few paired with corresponding passwords.

The rest of the activity was chatter among members of dark web and underground forums about possible techniques to exploit these apps or their user base, such as account checkers and brute forcers.

By the Numbers

Dark Web Markets (Listings of credentials and associated user data) — 77%

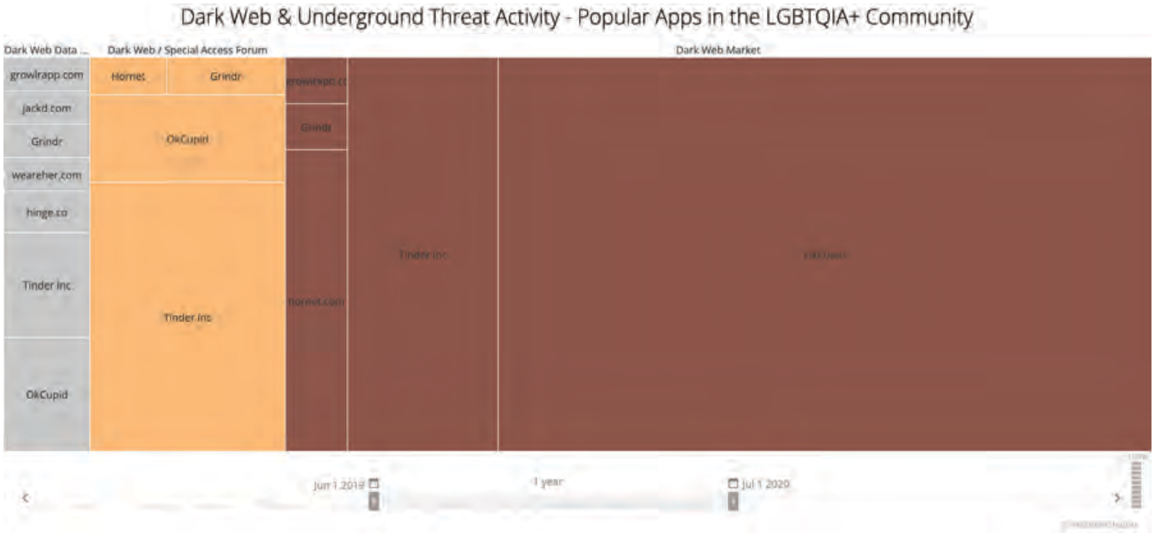
1. OkCupid
2. Tinder
3. Hornet
4. Grindr
5. Growlr

Dark Web/Underground Forum Chatter — 17%

1. Tinder
2. OkCupid
3. Grindr
4. Hornet

Data Dumps — 6%

1. OkCupid
2. Tinder
3. Hinge
4. HER
5. Grindr
6. Jack'd
7. Growlr



Source map of dark web/underground threat activity targeting popular apps in the LGBTQIA+ community (Source: Recorded Future)

International Targeting, Surveillance, and Censorship

Executive Summary

Recorded Future observed multiple instances of broadly defined cyberattacks (including targeted cyberattacks, censorship, and surveillance) targeting LGBTQIA+ communities and individuals in Russia and Eastern European nations. In Russia, state-supported advanced persistent threat (APT) groups have historically targeted domestic LGBTQIA+ communities, and other, unattributed intrusion activity impacted LGBTQIA+ activists in Ukraine. Surveillance and censorship was widespread across Russia and Eastern Europe with many nations passing restrictive legislative policies against open expression of LGBTQIA+ content online.

Members of the LGBTQIA+ community in the Middle East have been met with limited freedoms and protections against discrimination. While facing these limitations, the Middle Eastern LGBTQIA+ community has also endured online attacks (such as harassment, doxxing, and sextortion), surveillance, and censorship. In many countries, governments have used domestic telecommunications companies to block pro-LGBTQIA+ apps and websites. Further, Recorded Future has found that law enforcement and, very likely, intelligence agencies have deployed the use entrapment to expose members of the LGBTQIA+ community for imprisonment and torture.

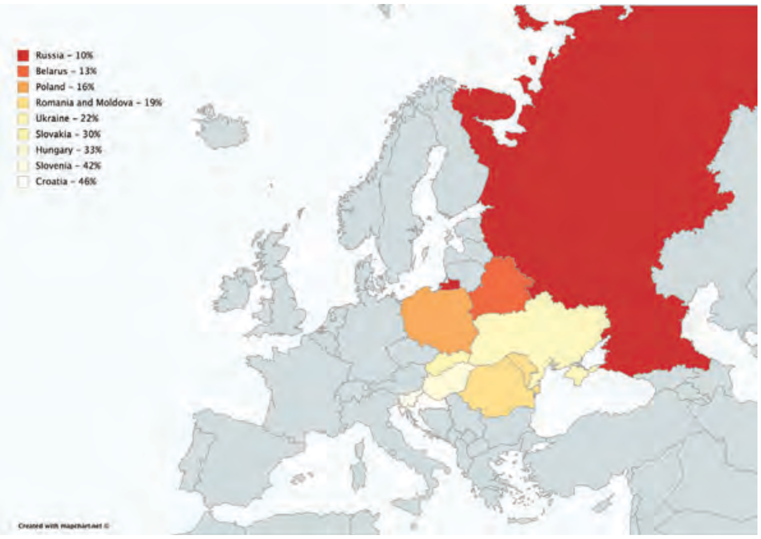
Similar activity was observed affecting LGBTQIA+ individuals in various Asian countries in the past five years, specifically Azerbaijan, China, Georgia, India, Indonesia, Malaysia, Myanmar, Pakistan, Singapore, South Korea, and Sri Lanka. Many of these attacks were instigated by the state for censorship or surveillance purposes, or by individual actors motivated by financial interests or social stigma.

Over the past decade, Latin America has been a bright spot for LGBTQIA+ rights, and the region now leads the Global South in terms of legal protections for the community. However, violence against the LGBTQIA+ community, albeit not state-directed, is still a significant issue, especially for transgender women, with a reported four LGBTQIA+ persons murdered every day in Latin America. The region's religious tradition and history of authoritarianism has kept much of the LGBTQIA+ community on the fringes of mainstream society, and many governments do not make a coherent effort to report or even respond to violence or other issues facing the community. The lingering social stigma towards the LGBTQIA+ community and the growing influence of evangelical Christian groups in Brazil and Central America pose the greatest threats to LGBTQIA+ rights in the region.

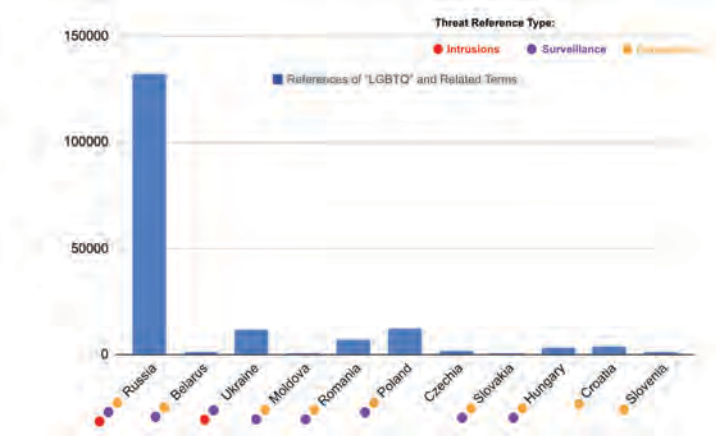
Across much of Africa, the LGBTQIA+ community is perceived as a threat to society that states are combating through organized crackdowns, surveillance, and censorship. In some instances, African governments are partnering with private sector surveillance organizations to target "high risk" groups, which includes the LGBTQIA+ community. Entrapment by law enforcement agencies and criminals is a common theme observed across Africa, with the outing of LGBTQIA+ individuals posing a significant threat due to strict anti-LGBTQIA+ legislation and socially conservative views among the public.

Country	Gender Change	Marriage Equality	Employment Discrimination	Housing Discrimination	Conversion Therapy
Russia	Legal	Illegal	Ambiguous	No Protection	Not Banned
Belarus	Legal	Unrecognized	No Protections	Ambiguous	Not Banned
Ukraine	Legal	Unrecognized	Protections Offered	Protections Offered	Not Banned
Moldova	Legal	Illegal	N/A	Protections Offered	Not Banned
Romania	Ambiguous	Unrecognized	Ambiguous	Protections Offered	Not Banned
Poland	Legal	Unrecognized	Limited Protections	Protections Offered	Not Banned
Czech Republic	Legal	Civil Unions	Protections Offered	Protections Offered	Not Banned
Slovakia	Ambiguous	Unrecognized	Protections Offered	Protections Offered	Not Banned
Hungary	Legal	Other Type of Partnership	Protections Offered	Protections Offered	Not Banned
Croatia	Legal	Civil Unions	Limited Protections	Protections Offered	Not Banned
Slovenia	Legal	Other Type of Partnership	Limited Protections	Limited Protections	Not Banned

The information found in the chart above is courtesy of Equaldex.
The term Illegal refers to countries where foreign same-sex couples are legal, but same-sex marriage is illegal.*



Map of Russia and Eastern Europe showing legal and policy practices supportive of LGBTQIA+ community (Ranked from 0% at worst to 100% at best, based on criteria like equality and non-discrimination; family; hate crime and hate speech; legal gender recognition and bodily integrity; civil society space; and asylum). (Sources: Mapchart & ILGA Europe)



Number of references to "LGBTQ" terms in Russia and Eastern European countries from the past five years (Source: Recorded Future)

Russia and Eastern Europe

Background

Russia and many Eastern European nations have limited the rights of LGBTQIA+ communities and maintained policies that censor, monitor, fine, or criminalize speech or outward displays of pride online. In June 2013, the Russian government approved a law limiting how information relating to lesbian, gay, bisexual, and transgender issues are shared, imposing fines and banning rallies or protests. On June 20, 2017, the regulation, colloquially known as the "gay propaganda law," was found by the European Court of Human Rights to be discriminatory and to serve no legitimate public interest. A report from Human Rights Watch indicates this law has led to increased social hostility against the LGBTQIA+ community and limited access to educational and support services for LGBTQIA+ youth.

In January 2020, Russian President Vladimir Putin announced further efforts to restrict rights in the LGBTQIA+ community by proposing a referendum which would effectively ban gay marriage. This proposal was couched amid several other potential changes to the Russian constitution, including an amendment which would allow for Vladimir Putin to remain president beyond his currently limited two consecutive terms. The proposal to codify marriage as a union between a man and a woman reportedly appeals to a populist audience, and the vote is set to occur from June 25 to July 1, 2020.

Moldova has sought to pass similar discriminatory measures as those in Russia. In May 2016, the Moldovan Socialist Party proposed a law, similar to the so-called "gay propaganda" measure, which sought to "impose fines for spreading 'homosexual propaganda' to minors 'through public meetings, the media, the Internet,' and other means." The legislation was ultimately abandoned in favor of obtaining an Association Agreement which would allow Moldova to gain entry into the European Union.

Other nations in Eastern Europe have also taken steps to limit the rights of LGBTQIA+ community members. The government of Belarus has led a campaign, supported by Russia, to block efforts by the United Nations to recognize LGBTQIA+ communities and stand against homophobia. ILGA-Europe conducted an assessment of human rights in Belarus between January and December 2019 and found that the nation received an overall low score of 13% in the freedoms and rights provided to individuals. An anecdotal account of life for a gay man living in Belarus revealed that he faced discrimination and had to conduct much of his relationship online due to homophobic attacks.

The Hungarian government has not granted full rights to the LGBTQIA+ community. Adoptions are allowed for LGBTQIA+ individuals but not same-sex couples, and same-sex couples cannot be married but can enter into a legal partnership. On May 19, 2020, however, the Hungarian government took regressive actions against the LGBTQIA+ community when the Hungarian Parliament voted in favor of prohibiting transgender individuals from changing their gender in official legal documents. Additionally, Hungarian authorities have not adequately afforded the LGBTQIA+ community the same protections as other citizens, with reports indicating that police in Hungary did not properly investigate or prosecute attacks against individuals.

On June 14, 2020, the BBC reported that in Poland, incumbent President Andrej Duda employed a homophobic platform in his re-election campaign that sought to "prevent gay couples from marrying or adopting children and to ban teaching about LGBTQIA+ issues in schools." In its report, the BBC cited international, independent LGBTQIA+ advocacy group IGLA-Europe as noting that Poland was among the worst nations in Eastern Europe for LGBTQIA+ rights. According to reporting from a Ukrainian LGBTQIA+ human rights group, online content in relation to the community was largely accurate in its usage of language (such as employing non-discriminatory language and not misgendering individuals) and neutral or positive in their depictions with only 4% negative coverage observed in an assessment of "16 popular online media [sources] in the period from 12 to 18 June 2019."

Same-sex marriage is not recognized in Poland, Slovakia, Belarus, Ukraine, or Romania, and many couples face discrimination in those nations. A report from July 16, 2019, revealed that couples in Romania faced hostility and discrimination; a survey from the Romanian Institute for Evaluation and Strategy conducted between November and December 2018 revealed that more than half of those polled either mistrust, do not accept, or refuse to be friends with someone from the LGBTQIA+ community. The reporting attributes much of the homophobia to the influence of the Romanian Orthodox Church, which supported a failed referendum in October 2018 to impose restrictions on marriage in the country.

Targeting

According to open source reporting from March 2019, the cybersecurity company FireEye has indicated that the Russian advanced persistent threat (APT) groups APT28 and Sandworm had targeted Russian domestic political LGBTQIA+ opposition groups. A November 2019 report by Wired revealed that the Sandworm targeting of LGBTIA+ activists was identified by FireEye when similarities were found between malicious phishing documents used in the targeting of the activists and those against the Pyeongchang Winter Olympics in February of 2018. According to the reporting, both sets of documents, including files from other intrusions against Ukraine and Spiez Laboratory by Sandworm, had all been created using the Malicious Macro Generator public tool and all shared related metadata information. A report from Google's Threat Analysis Group (TAG) indicated that the targeting activity against the Russian LGBTQIA+ activists occurred in June 2017. Although the lure documents or phishing messages used in the Sandworm activity, or material associated with previously referenced APT28 operations, are not currently available, it is nevertheless likely that they represent a component of espionage or hack and leak efforts by these groups, as both typically engage in such actions.

Intrusions against LGBTQIA+ organizations were also reported outside of Russia. A report from the Ukrainian LGBTQIA+ Human Rights organization "NASH MIR" indicated that, in 2019, online intrusions aimed at an unspecified number of unidentified, public LGBTQIA+ organizations coincided with public LGBTQIA+ events. No attribution or indicators were provided in relation to the activity and it is not possible to determine whether these efforts originated from domestic or foreign intrusion actors or whether this activity was the result of cybercriminal, hacktivist, nationstate, or other entities.

Surveillance

An open source report from October 6, 2013, indicated that the Russian government had planned to disrupt any potential protest activity in support of LGBTQIA+ rights ahead of the 2014 Winter Olympics at Sochi, Russia. According to the article, "Using DPI, Russian authorities will be able to identify, tag and follow all visitors to the Olympics, both Russian and foreign, who are discussing gay issues, and possibly planning to organize protests." DPI refers to deep packet inspection (DPI) technology very likely inherent within the Russian System for Operative Investigative Activities (SORM to track both Russian citizens and foreign visitors to the Games. SORM is used by both the Federal Security Services (FSB) and Ministry of Internal Affairs (MVD) for domestic surveillance.

The 2014 Winter Olympics were not the only sporting events in which the Russian government very likely conducted domestic surveillance employing DPI monitoring. A July 3, 2019, report indicated that the Federal Security Service (FSB) and domestic law enforcement also likely monitors events organized by the Russian LGBTQIA+ Sport Federation under the guise of providing "protection" to football (soccer) fans. Organizers of the event indicate that the LGBTQIA+ community has been surveilled and harassed by domestic law enforcement as part of an effort to enforce the "gay propaganda" law, resulting in blackmail, assault, data gathering, and other aggressive efforts against the LGBTQIA+ community in Russia.

Censorship

Censorship of LGBTQIA+ content is predominant in Russia, following the passage of the "gay propaganda" law in 2013. Efforts to limit speech relating to the LGBTQIA+ community has impacted popular, international films. In June 2019, the Russian government announced its plans to censor the Elton John biopic "Rocketman" by removing all references to the singer's relationship with his husband David Furnish, resulting in John issuing a letter directly to Russian President Vladimir Putin calling out hypocrisy in the domestic policies which attempt to erase the depiction of love in the LGBTQIA+ community. Despite the direct appeals, censorship remains ongoing and on February 28, 2020, reports indicated that efforts were aimed at the popular Disney Pixar film "Onward" when references to a lesbian character's girlfriend were edited out of the movie.

Blocking of LGBTQIA+ content in Russia extends beyond film to online video content on YouTube. On November 15, 2019, Human Rights Watch reported that the Russian Ministry of the Interior (MVD) charged Maksim Pankratov with "propaganda of non-traditional sexual relations" for his participation in the YouTube video series "Real Talk" which presents a discussion between Maksim and children ages six to 13 about his life as a gay man. Additionally, the Investigative Committee of Moscow attempted to charge Maksim with sexual assault against the children in the video. In conjunction with the charges, the Russian Internet Watchdog Roskomnadzor blocked the video on domestic networks. Human Rights Watch also indicated that Maksim received online threats of physical violence from Russian citizens who, although unable to view the blocked video, believed he had assaulted the children due to the charges.

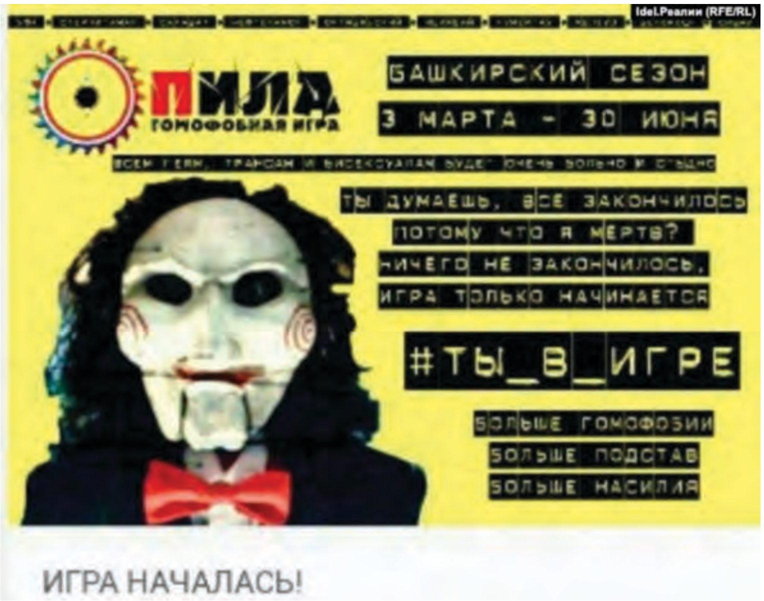
In addition to film and online media censorship, a festival in the Russian far-east city of Komsomolsk-on-Amur was cancelled in March 2019 because authorities were concerned that the planned performance of "Blue and Pink" would promote an LGBTQIA+ agenda and therefore be in violation of the 2013 “gay propaganda” law. The cancellation was announced via social media and came as part of a likely broader campaign against the organizer of the festival, female artist and LGBTQIA+ activist Yulia Tsvetkova, who was arrested and charged in late 2019 with distributing pornography after creating female body-positive art. Yulia has come under attack from online hate groups like “Saw,” which her family has reported to the Russian Main Directorate of the Ministry of Internal Affairs, but the government has afforded her no protection. A report from Amnesty International from December 11, 2019 indicated that Yulia has been fined and is currently under house arrest for her activism and art.

Doxxing and Online Stalking

According to a May 5, 2018 report by Radio Free Europe/Radio Liberty (RFE/RL), members of the LGBTQIA+ community in the Bashkortostan region in Southwestern Russia were targeted under a social media campaign named “ПИЛА” (lit. PILA, “SAW,” named after the eponymous U.S. horror films), which exists as a “a self-declared anonymous network of anti-gay activists.” The campaign announced that between March 3 and June 30, in the Bashkortostan capital city of Ufa, that “a hunt” would commence for LGBTQIA+ individuals, promising, “more homophobia, more frame-ups, more violence.” The campaign threatened to import “more than 50 of Chechnya’s best homophobes” to participate. The report further outlines an attack of a man living in Ufa, who was assaulted by two men after connecting in an online chat.

Activity associated with this campaign is likely to have persisted despite at least one government takedown of online resources promoting it. The ongoing nature of this activity is evidenced by a further September 18, 2019 report by RFE/RL that describes the brutal 2019 killing of prominent LGBTQIA+ activist Yelena Grigoryeva in St. Petersburg. Days before her murder, the “SAW” group posted information about Grigoryeva on its site, indicating that she was likely a victim of this campaign.

On September 24, 2019, Reuters reported that in addition to its own website, the group had employed a number of platforms, including Instagram, Telegram, and the Russian social media platform VK to terrorize members of the LGBTQIA+ community by issuing threats and disseminating homophobic posts online. A lack of accountability and the ability for this group to persist online has created an atmosphere of hostility to the LGBTQIA+ community and led people to flee the country. Rights activist Nikita Tomilov indicated that he left Russia following threats consisting of “photos of mutilated bodies with the warning ‘you’re next,’” as well as the presence of unidentified surveillance personnel outside his home.

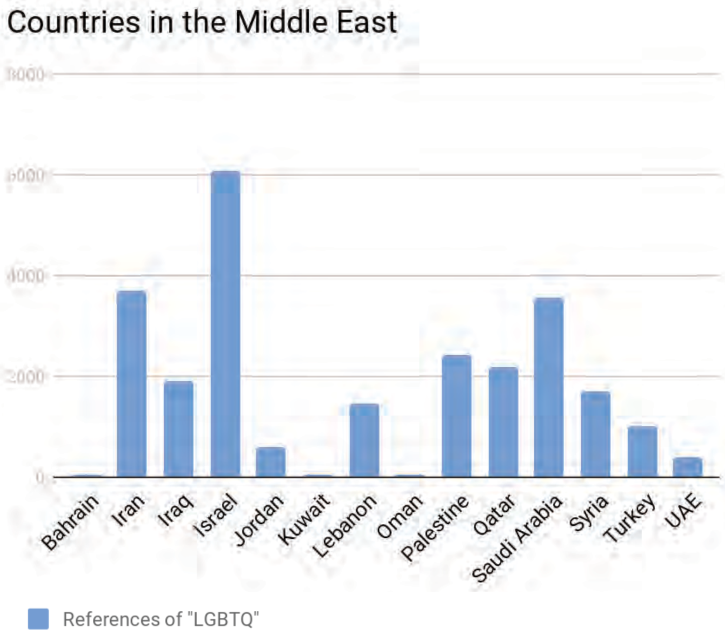


Screenshot of the initial “SAW” online posting (Source: RFE/RL)

Middle East

Background

This section is dedicated to identifying nation-state activity in the Middle East, which in this report includes the following countries: Bahrain, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, and the United Arab Emirates (UAE). For this study, Recorded Future specifically focused on the time frame of 2015 to 2020. To analyze reported threats against the LGBTQIA+ community in the Middle East, analysts constructed a query that searched against Recorded Future’s collection on dark web and underground forums, social media, mainstream media, academic journals, and security vendor reporting. In addition to this, Recorded Future also researched nation-state threats using OSINT techniques.



Number of references to the term “LGBTQ” in Middle Eastern countries from the past 5 years. (Source: Recorded Future)

Country	Homosexuality	Gender Change	Marriage Equality	Employment Discrimination	Housing Discrimination	Conversion Therapy
Bahrain	Ambiguous	Legal	Illegal	No Protections	No Protections	Not banned
Iran	Illegal	Legal	Illegal	No Protections	Ambiguous	Not banned
Iraq	Ambiguous	Ambiguous	Illegall	No Protections	No Protections	Ambiguous
Israel	Legal	Legal	Illegal*	Some Protections	Some Protections	Ambiguous
Jordan	Legal	Legal	Illegal	No Protections	No Protections	Ambiguous
Kuwait	Illegal	Illegal	Illegal	No Protections	No Protections	Ambiguous
Lebanon	Ambiguous	Legal	Illegal*	Some Protections	No Protections	Not banned
Oman	Illegal	Illegal	Illegal	Ambiguous	No Protections	Ambiguous
Palestine	Illegal	N/A	Illegal	No Protections	No Protections	Not banned
Qatar	Illegal	Illegal	Illegal	No Protections	No Protections	Ambiguous
Saudi Arabia	Illegal	Illegal	Illegal	No Protections	No Protections	Ambiguous
Syria	Illegal	Legal	Illegal	Varies by Region	Varies by Region	Ambiguous
Turkey	Legal	Legal	Illegal	Ambiguous	No Protections	Not banned
UAE	Illegal	Illegal	Illegal	No Protections	No Protections	Not banned

The information found in the chart above is courtesy of Equaldex.
The term Illegal refers to countries where foreign same-sex couples are legal, but same-sex marriage is illegal.*

Throughout the Middle East, countries have enacted laws regarding the legality of homosexuality. In some countries, governments have inherited strict laws from European colonies that banned homosexuality. In other countries, such as Saudi Arabia, anti-LGBTQIA+ laws are derived from a country's interpretation of Sharia law.

As seen in the table below, members of the LGBTQIA+ community in the Middle East have limited freedoms and protections against discrimination. In a majority of Middle Eastern countries, homosexuality is illegal, and in every Middle Eastern country, same-sex marriage is barred. In addition to these limitations, members of the LGBTQIA+ community face online harassment, surveillance, and censorship.

In some instances, nation states have leveraged their power and influence over telecommunication companies to shut down LGBTQIA+ applications and block websites.

Targeting

According to a February 2020 report by the Jerusalem Post, members of the Israeli LGBTQIA+ community have been subject to a 36% rise in online harassment since 2018. The term "harassment" encompasses hate speech and violence against the LGBTQIA+ community. The Jersualem Post noted that there was a 58% rise in online harassment following statements made by Education Minister and Bayit Yehudi leader Rafi Peretz, who stated that "conversion therapy can be performed on those of LGBTQIA+ orientation."

In Iraq and Turkey, Recorded Future identified reports that claimed members of the LGBTQIA+ community were the cause of COVID-19 in both countries. From a March 2020 report, the Jerusalem Post published claims by Iraqi Shi'ite cleric leader Muqtada al-Sadr, who stated that the legalization of same-sex marriage was the catalyst for the spread of COVID-19. Similarly, in May 2020, the Guardian reported on efforts by the Turkish government to place blame on the LGBTQIA+ community for the COVID-19 pandemic.

In a 2018 report, SMEX found that members of the Lebanese LGBTQIA+ community were vulnerable to online threats such as blackmail, sextortion, and doxxing. All three of these threats centered around the non-consensual sharing of intimate images that were meant to "out" members of these communities. From their study, SMEX researchers noted that "the number of cases in Lebanon has grown in recent years, with the Internal Security Forces (ISF) issuing more warnings each year. In 2016, Joseph Moussallem, a colonel at the ISF's Cybercrime and Intellectual Property Bureau, reported that it received 346 total complaints of online 'sextortion' and by early 2017 it was receiving complaints "practically every day."

Surveillance

In a 2018 study by Article 19, researchers noted that nation-state actors were using fake social media accounts to track members of the LGBTQIA+ community, entrap them, and ultimately subject these individuals to arrest, blackmail, or degrading acts. From the Article 19 study, fake online account activity was prevalent in countries such as Lebanon and Iran, where nation-state actors infiltrated social apps and messaging platforms like Telegram to track LGBTQIA+ members. In Lebanon, citizens have been subjected to phone searches at military and police checkpoints. From their searches, police and military members have been known to look for social media or chat apps that are popular among the LGBTQIA+ community.

These tactics have been used historically as well. In 2012, Saudi Arabia's religious police (the Committee for the Propagation of Virtue and the Prevention of Vice) arrested a man who was using Facebook to find male romantic partners. A year later, according to the Electronic Frontier Foundation (EFF), Saudi police "entrapped [another male] in a public chatroom." The male was lured into meeting with police with his drag outfits and makeup; once apprehended and arrested, he was jailed and tortured. In 2014, it was alleged that Israeli intelligence operatives identified gay Palestinians via online and phone surveillance for the purpose of turning these males into Israeli operatives.

Censorship

Like many countries around the world, Recorded Future has found that Middle Eastern countries have censored the LGBTQIA+ community through the blocking of social media and social apps. In May 2019, the dating app Grindr was blocked from users in Lebanon. Lebanese telecommunications companies Ogero and Touch blocked 3G and 4G access to the app, according to their social media posts. In the case of Ogero, the Lebanese local newspaper the Daily Star reported that the company shut down access to Grindr "on the orders of the public prosecutor's office." In Turkey, TikTok moderators were advised to censor LGBTQIA+ content, specifically videos that depict "intimate activities (holding hands, kissing, touching) between homosexual lovers." These guidelines and blocks to content were later revised after public backlash.

In addition, countries have also censored the LGBTQIA+ community through blocking pro-LGBTQIA+ websites. In Jordan, the government has been known to block news sites and other sources of information that push content related to the Jordanian LGBTQIA+ experience. In the 2019 Freedom of the Net study for Jordan, Freedom House noted that "in 2017, the Media Commission reissued an order to block access to the local LGBTQIA+ online magazine My.Kali, after an Islamist member of Parliament, Dima Tahboub, requested an inquiry into the site." Along the same lines, the government in the UAE has also blocked pro-LGBTQIA+ websites such as the LGBTQIA+ sports new site, Outsport, as well as the website for the International Lesbian, Gay, Bisexual, Trans, and Intersex Association.

Asia

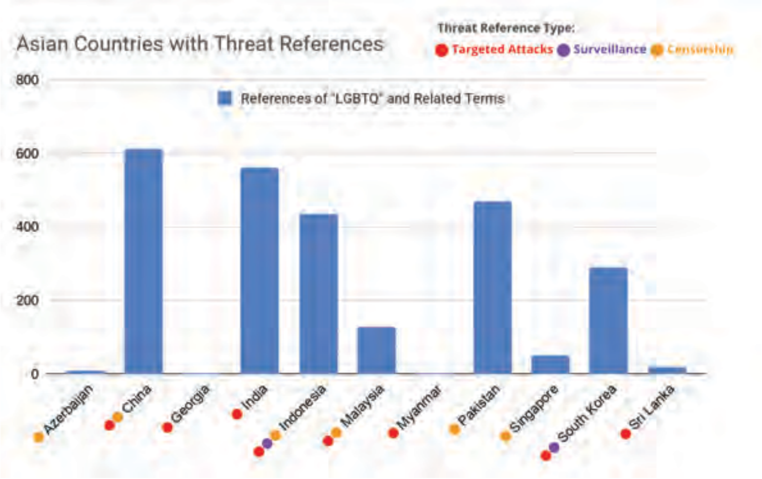
Background

Recorded Future observed a total of 3,091 references to LGBTQIA+ and similar keywords ('gay', 'lesbian', 'queer', 'transgender', 'homosexual') in relation to 31 Asian countries within the last five years across open sources. The countries were: Armenia, Azerbaijan, Bangladesh, Bhutan, Brunei, Cambodia, China, Georgia, India, Indonesia, Japan, Kazakhstan, Kyrgyzstan, Laos, Malaysia, Mongolia, Myanmar, Nepal, North Korea, Pakistan, Philippines, Singapore, South Korea, Sri Lanka, Taiwan, Tajikistan, Thailand, East Timor, Turkmenistan, Uzbekistan, and Vietnam.

When specifically querying for cyber events involving LGBTQIA+ and Asian countries, we did not identify references to named threat actors or threat groups that have targeted the LGBTQIA+ community. However, we did observe multiple instances of broadly defined cyberattacks (including targeted cyberattacks, censorship, and surveillance) targeting LGBTQIA+ communities and individuals in various Asian countries in the past five years, specifically Azerbaijan, China, Georgia, India, Indonesia, Malaysia, Myanmar, Pakistan, Singapore, South Korea, and Sri Lanka. Many of these attacks were instigated by the state or individual actors motivated by financial interests or social stigma.

Asia is home to countries that have some of the harshest LGBTQIA+ laws in the world, as well as countries that have recently passed some of the most progressive ones. Taiwan legalized same-sex marriage in 2019 while governments and the public in Japan and China have expressed support for similar measures.

According to a December 2019 report by the IILGA, same-sex sexual acts are criminalized in 10 Asian countries, specifically Bangladesh, Bhutan, Brunei, Malaysia, Myanmar, Pakistan, Singapore, Sri Lanka, Turkmenistan, and Uzbekistan. However, despite the legality of same-sex sexual acts in 18 other Asian countries, members of the LGBTQIA+ community largely face discrimination and oftentimes harassment and violence.



Number of references to the term "LGBTQ" and related terms in select Asian countries from the past five years (Source: Recorded Future)

The patriarchal and conservative nature of many Asian cultures and the shared emphasis on "family shame" create an additional layer of pressure and secrecy for the LGBTQIA+ community that differs from other regions of the world. The collectivist nature of many Asian cultures, which value interdependence, social harmony, and group cohesion, result in the experience of shame not only individually but also collectively — members of a community often experience shame in response to something that someone close to them has done. Relatedly, a report by Reuters found that LGBTQIA+ people in Asia often face violence from their own family members attempting to force them to conform to social norms.

Targeting

Recorded Future identified cyber-related targeted attacks on the LGBTQIA+ community in Asian countries including doxxing, blackmailing, and extortion of users of gay social apps, boycotting of LGBTQIA+-friendly services, and distributed denial of service (DDoS) attacks on gay websites.

The majority of cyber-related targeted attacks, however, were cases of cyberbullying and online harassment. Examples include cyber violence against LGBTQIA+ individuals in Sri Lanka, far-right Facebook pages disseminating anti-LGBTQIA+ narratives leading up to the first-ever Tbilisi Pride event in Georgia, online harassment of Malaysian LGBTQIA+ activist Numan Afifi following his speech at the UN Human Rights Council about LGBTQIA+ rights in Malaysia, and cyberbullying suffered by members of the LGBTQIA+ community in Myanmar.

Another type of cyber-related targeted attack is financially motivated and exploits the secrecy and societal pressure that members of the LGBTQIA+ community face for financial gain. Catfishing on gay social apps has increased in India, with online predators pretending to be gay (often using another person's photo) and luring innocent users into interaction before blackmailing them for money. Victims are sometimes beaten and sexually abused. In a 2008 attack, more than 10 gay websites and online chat rooms in China suffered DDoS attacks and had their databases wiped. The threat actor stopped the attacks once they received their requested payout. Although the attacks were reported to local police, cases were never filed.

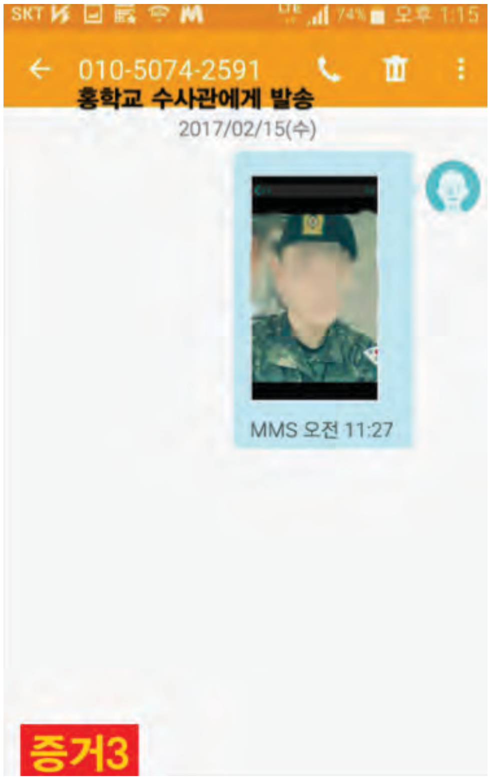
More recently, the LGBTQIA+ community in South Korea have faced significant anti-gay backlash from Korean society due to new COVID-19 cases being traced to customers of a popular gay club in Seoul. Not only has online hate speech against the LGBTQIA+ community increased, South Korean media outlets have also reportedly exposed the identities of gay club customers. There were also rumors that YouTubers joined gay social apps to out gay men live. Similar fears of being outed against their will in a society that harbors strong anti-gay sentiment exist in Japan, where LGBTQIA+ individuals fear that the government's contact tracing of COVID-19 patients could expose their identities.

Attacks have also targeted LGBTQIA+ allies. In October 2018, social media users in Indonesia launched the #UninstallGojek campaign against local ride-hailing app Gojek after a company executive published a social media post supporting the company's diversity and inclusion initiative which supported the LGBTQIA+ community. Many social media users reacted by posting screenshots of themselves uninstalling the Gojek app from their phones to protest the perceived approval of homosexuality by Gojek.

The majority of cyber-related targeted attacks observed by Recorded Future were conducted by non-state actors and motivated by financial interests, social stigma, and homophobia.

Surveillance

Recorded Future identified three instances of governmental surveillance targeting the LGBTQIA+ community in Asia during the past five years. In 2017, the Military Human Rights Center for Korea (MHRCK) revealed that the South Korean military compiled a blacklist of gay soldiers, and in some cases coerced gay soldiers to provide the names and photos of other gay soldiers.



010-5074-2591
홍학교 수사관에게 발송

2017/02/15(수)

MMS 오전 11:27

Screenshot of a message thread in which a gay soldier was asked to send a military investigator a screenshot of a fellow gay soldier captured from gay dating app Jack'd (Source: Korea Expose)

Additionally, we observed the Indonesian government and Azerbaijan police using surveillance software sold by Israel's Verint Systems to track and profile LGBTQIA+ activists and members of the LGBTQIA+ community. According to Israeli media outlet Haaretz, Verint products were used to create a database of LGBTQIA+ rights activists who had been targeted for surveillance. It is worth noting that homosexuality is not a crime in either country.

Censorship

The two Asian countries that had the most prominent censorship instances observed by Recorded Future in the past five years were China and Indonesia, where LGBTQIA+ social apps were banned and LGBTQIA+-related websites taken down without public explanation. Other censorship or self-censorship instances have been observed in Pakistan, Malaysia, and Singapore, where LGBTQIA+ dating sites and news sites have been made unavailable or charges have been filed towards bloggers who wrote about issues such as discrimination against LGBTQIA+ people.

While homosexuality has been decriminalized in China since 1997, instances of Chinese censorship targeting the LGBTQIA+ community are rampant, including:

- The May 2017 shutdown of Rela, China's leading lesbian app with over 5 million registered users. The app is no longer available on Apple's App Store, and its website and social media accounts have also been taken down. Another Chinese dating app for gay people, Zank, was also shut down in April 2017.
- A July 2017 regulation banning online content that features "abnormal" sexual activity, including portrayals of homosexuality, prostitution, and drug addiction. Online video platforms are required to hire at least three "professional censors" to review content.
- In April 2018, Chinese social media platform Weibo announced a ban on homosexual content to "create a sunny and harmonious community environment." The decision was swiftly reversed amid outcry from millions of Weibo users.
- A July 2018 ban of computer game The Sims FreePlay because players can engage in same-sex interaction and make their characters gay in the game.
- A March 2020 blocking of prominent fanfiction website Archive of Our Own (AO3), known for featuring many stories that include same-sex relationships. Other bloggers of queer content have taken to self-censorship in light of the recent tightening of China's internet censorship controls.

The Indonesian government has also engaged in censorship amid the rise of anti-gay sentiment in the country, despite the legality of homosexuality in the country:

- In February 2016, the Indonesian government asked popular messaging app LINE to remove same-sex emojis to preempt "public unrest."
- In 2017, the Ministry of Communication and Information (MCIT) blocked the LGBTQIA+ dating app Grindr, and in January 2018, blocked another gay dating app known as Blued.52.
- In October 2018, an Indonesian man was arrested for managing a Facebook page for the LGBTQIA+ community. He was charged with violating Indonesia's electronic information law.

Latin America

Background

Recorded Future observed a total of 244,168 references to the LGBTQIA+ community[1] and 7,369 references to violence[2] and the LGBTQIA+ community in relation to the 20 largest Latin American countries[3] over the past five years. When specifically querying for cyber events involving LGBTQIA+ and Latin America, we did not identify references to any named threat actors or threat groups that have targeted the LGBTQIA+ community.

Latin America has made significant progress regarding LGBTQIA+ rights over the past decade, and now leads the Global South in legal protections for the LGBTQIA+ community. For example, no Latin American country criminalizes homosexual activity, and six out of the 10 most populous have legalized either same-sex marriage or same-sex unions. Anti-discrimination laws for LGBTQIA+ people are also making enormous gains in the region, with the majority of countries offering limited-to-full protection against employment and housing discrimination.

However, despite the substantial legal progress made for LGBTQIA+ rights in Latin America, significant issues remain. For example, in 2019, a coalition of LGBTQIA+-focused nonprofits released a report that found, on average, four LGBTQIA+ people are murdered every day in Latin America, with Colombia, Honduras, and Mexico accounting for more than 90% of cases. While those three countries have a history of drug-related violence, the report pointed to the region's historical exclusion of the LGBTQIA+ community, lingering social stigma, and a lack of coherent institutional response for the continued violence against the community. The issue is exacerbated by the emerging political backlash in several Latin American countries to the progress made for LGBTQIA+ rights.

Country	Homo-sexuality	Gender Change	Marriage Equality	Employment Discrimination	Housing Discrimination	Conversion Therapy
Argentina	Legal	Legal	Legal	Varies by Region	Varies by Region	Banned
Bolivia	Legal	Legal	Unrecognized	Protections Offered	Protections Offered	Not Banned
Brazil	Legal	Legal	Legal	Protections Offered	Varies by Region	Banned
Chile	Legal	Legal	Civil Unions	Protections Offered	Protections Offered	Not Banned
Colombia	Legal	Legal	Legal	Limited Protections	Limited Protections	Not Banned
Costa Rica	Legal	Legal	Unrecognized	Protections Offered	Protections Offered	Not Banned
Cuba	Legal	Legal	Unrecognized	Protections Offered	Protections Offered	Not Banned
Dominican Republic	Legal	Ambiguous	Unrecognized	Protections Offered	Protections Offered	Not Banned
Ecuador	Legal	Legal	Civil Unions	Limited Protections	Protections Offered	Banned
El Salvador	Legal	Ambiguous	Unrecognized	Protections Offered	Protections Offered	Ambiguous
Guatemala	Legal	Legal	Unrecognized	Limited Protections	Limited Protections	Not Banned
Haiti	Legal	Legal	Illegal	Ambiguous	No Protections	Not Banned
Honduras	Legal	Ambiguous	Illegal	Protections Offered	Protections Offered	Not Banned
Mexico	Legal	Legal	Legal	Protections Offered	Protections Offered	Banned
Nicaragua	Legal	Ambiguous	Unrecognized	Protections Offered	Protections Offered	Not Banned
Panama	Legal	Legal	Unrecognized	Limited Protections	No Protections	Not Banned
Paraguay	Legal	Ambiguous	Unrecognized	No Protections	No Protections	Not Banned
Peru	Legal	Illegal	Unrecognized	Protections Offered	Protections Offered	Not Banned
Uruguay	Legal	Legal	Legal	Protections Offered	Protections Offered	Not Banned
Venezuela	Legal	Ambiguous	Unrecognized	Limited Protections	Ambiguous	Not Banned

The information found in the chart above is courtesy of Equaldex.
The term Illegal refers to countries where foreign same-sex couples are legal, but same-sex marriage is illegal.*

[1] Including "gay", "lesbian", "queer", "transgender", and "homosexual".

[2] English, Spanish, and Portuguese linguistic variations of the terms "attack" and "murder"

[3] Brazil, Mexico, Colombia, Argentina, Peru, Venezuela, Chile, Ecuador, Guatemala, Cuba, Bolivia, Haiti, Dominican Republic, Honduras, Paraguay, Nicaragua, El Salvador, Costa Rica, Panama, Uruguay

The United Nations' independent expert on sexual orientation and gender identity, Victor Madrigal-Borloz, has warned against the growing social and political influence of evangelical Christian groups in Latin America, particularly in Brazil and Central America. Many of these groups, which receive support and coaching from counterparts in the United States, hinder efforts to promote social awareness of LGBTQIA+ issues and instead promote anti-LGBTQIA+ campaigns. For example, the growing influence of evangelical Christian groups is leading to the success of far-right politicians, such as Brazil's President Jair Bolsonaro, who refers to himself as a "proud homophobe," and Costa Rica's Fabricio Alvarado Muñoz, who reached second place in the country's presidential election running on an anti-LGBTQIA+ platform.

Targeting

Despite Latin America's history of authoritarianism and political corruption, little, if any, of the violence targeting the LGBTQIA+ community is the result of a state-coordinated effort in the past five years. However, LGBTQIA+ activists and politicians face a rising number of homophobic and transphobic attacks, especially in Brazil and Central America.

In Brazil, an openly gay member of congress, Folha de S. Paulo, forfeited his seat and fled the country after receiving a large number of death threats online in 2019. Paolo claimed that the death threats intensified after a fellow LGBTQIA+ politician Marielle Franco was allegedly assassinated in 2018. In Mexico, several notable LGBTQIA+ activists were murdered over the past three years, including pioneering LGBTQIA+ activist Oscar Cazorla, who was found murdered in his home in Oaxaca, Mexico in 2019, and three LGBTQIA+ activists who were kidnapped and found murdered outside Mexico City in 2018.

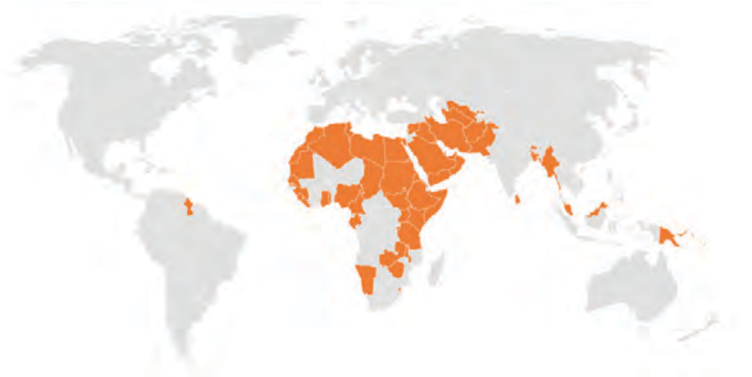
Many of the attacks against the LGBTQIA+ community go uninvestigated or unreported in Latin America, which makes reports and surveys conducted by organizations like Sin Violencia all the more critical in the region. For example, a survey conducted in Brazil, which relied on news and social media reports instead of the country's official crime statistics, found that 343 LGBTQIA+ people, or one person every 25 hours, were murdered in 2016. Another survey, conducted by Amnesty International in 2017, found that 88% of LGBTQIA+ people seeking asylum from the Northern Triangle[4] suffered sexual or gender-based violence in their country of origin. The violence is then made all the more real in cases like the 2019 murder of a transgender woman in El Salvador after she was rejected for asylum in the United States and subsequently deported.

Africa

Background

According to the International Lesbian, Gay, Bisexual, Trans and Intersex Association's December 2019 report, there are 70 countries around the globe where same-sex sexual acts are either illegal or defacto illegal, and a significant proportion (47%) of those countries are in Africa, where same-sex sexual acts are criminalized more than any other continent. Same-sex sexual acts are only legal in 21 out of the 54 countries on the African continent and, even in those countries where same-sex sexual acts are legal, only eight countries in Africa have any degree of protection against discrimination.

Homosexuality has been described in Africa as being a "Western import" and "un-African," but it might be more accurate to say that the criminalization of homosexuality is the Western import; anti-LGBTQIA+ laws that exist in the African continent today are largely imported from the British Commonwealth during the colonial era. In fact, there's a strong correlation between countries that were formerly under British rule and those that still criminalize homosexuality. In Africa, there was no criminal persecution of LGBTQIA+ individuals because of their sexuality, nor were there any homophobic, biphobic or transphobic laws prior to colonialization.



Countries where same-sex sexual acts are illegal (Source: ILGA World Report)

It's important to note that the criminalization of same-sex sexual acts only applies to men in some African countries, namely Eswatini (formerly known as Swaziland), Kenya, Mauritius, Namibia, Sierra Leone, Togo, and Zimbabwe. Most of these countries were former British colonies, and their lack of legislation criminalizing same-sex sexual acts between women may also be inherited from the colonial era. For example, lesbianism was never illegal in the U.K., and when an attempt to criminalize lesbianism was introduced in U.K. Parliament, it was rejected because politicians thought an extreme few were lesbians and that enacting a law would draw attention to lesbianism and could encourage women to explore it.

Homophobic, biphobic, and transphobic legislation in Africa has a hugely damaging and sometimes deadly impact on the LGBTQIA+ community. The maximum penalty for same-sex sexual acts in four African countries is the death penalty, while eight African countries have a prison sentence of 10 years or more. There are many examples of state crackdowns on the LGBTQIA+ community in Africa, but other threats faced by the LGBTQIA+ community in Africa include discrimination and violence from other members of the public, targeting by criminals for extortion and theft, and even a health crisis where harsh laws are resulting in thousands of gay men dying each year from HIV-related illnesses.

Nevertheless, there's room for hope. South Africa has legal protections and recognition of LGBTQIA+ individuals in place. Botswana's High Court unaninmously

[4] Northern Triangle includes El Salvador, Guatemala, and Honduras

decriminalized homosexuality in June 2019, arguing that the colonia-era law was unconstitutional, despite Botswana's government then appealing the decision. Even in the face of adversity, the LGBTQIA+ community are coming together to campaign for basic human rights. Activists are training the LGBTQIA+ community on how to digitally protect themselves from law enforcement, state surveillance, and entrapment. Individuals are warning others about criminals targeting the LGBTQIA+ community through social and dating apps, naming attackers, and even uniting to organize "queermas" to combat loneliness in countries where being LGBTQIA+ can mean being shunned by family.

Targeting

Egyptian security forces under President Abdel Fattah al-Sisi launched their latest crackdown against the LGBTQIA+ community following some audience members waving pride rainbow flags at a concert in Cairo, hosted by a Lebanese band with an openly gay singer in September 2017. By mid-October, it was reported that over 60 men and women had been arrested under various laws against debauchery and promoting sexual deviancy, with a 1960s anti-prostitution law prohibiting immorality and debauchery making same-sex sexual acts de facto illegal. Tragically, a lesbian woman named Sarah Hegazi, who was arrested and tortured after waving a pride rainbow flag at the concert, has recently committed suicide during Pride Month in 2020.

Multiple online methods were used by security forces to identify, expose, and arrest members of the LGBTQIA+ community during the crackdown. One such approach was the monitoring of social media to identify individuals waving pride rainbow flags at the concert through video footage, with one person allegedly being arrested for posting positively about the concert on Facebook, sparking fear amongst other members of the LGBTQIA+ community with some subsequently deleting content from social media and social apps.

Another approach used by security forces involved using social and dating apps and online chat rooms to identify and entrap LGBTQIA+ individuals, which is reported as being a common policing technique used against the LGBTQIA+ community in Egypt. Furthermore, a network of Egyptian LGBTQIA+ advocacy organizations contacted Access Now's Digital Security Helpline to ask for their assistance in removing a fake Facebook page publishing content in their name, which could have been used by security forces to identify additional members of the community. A final, significantly more sophisticated approach that was likely used to identify members of the LGBTQIA+ community is the use of deep packet inspection (DPI) to monitor the online communications of the LGBTQIA+ community in Egypt; this is explored in more detail below in the 'surveillance' section of this report.

The motivations behind the Egyptian state crackdowns on the LGBTQIA+ community over the past several years are likely to maintain and garner public support of the President Abdel Fattah al-Sisi's regime. President al-Sisi was the prominent figure in the military coup that ousted an Islamist president in 2013 and, at the time, a Pew Research poll showed that 95% of Egyptians viewed homosexuality as unacceptable in society. Within the first few years of al-Sisi's regime, the number of LGBTQIA+ people arrested quadrupled and Egypt's security forces would widely publicize their raids on the LGBTQIA+ community across news networks. The repeated crackdowns on the LGBTQIA+ community are likely an attempt by President al-Sisi's regime to prove that they will continue to uphold conservative religious values in Egypt despite deposing an Islamist president, which is a popular stance among Egypt's mostly conservative population of both Christians and Muslims, who consider homosexuality to be a sin. For the government, the crackdowns have been an effective tool in distracting the population from blaming the regime for Egypt's political and economic woes.

FANS OF THE LEBANESE GROUP MASHROU LEILA SHOW A RAINBOW FLAG AT THEIR CONCERT IN CAIRO ON SEPTEMBER 22. PHOTO BY BENNO SCHWINGHAMMER/PICTURE-ALLIANCE/DPA/AP IMAGES

Pride rainbow flags at Mashrou Leila's concert in Cairo, 22 September 2017.

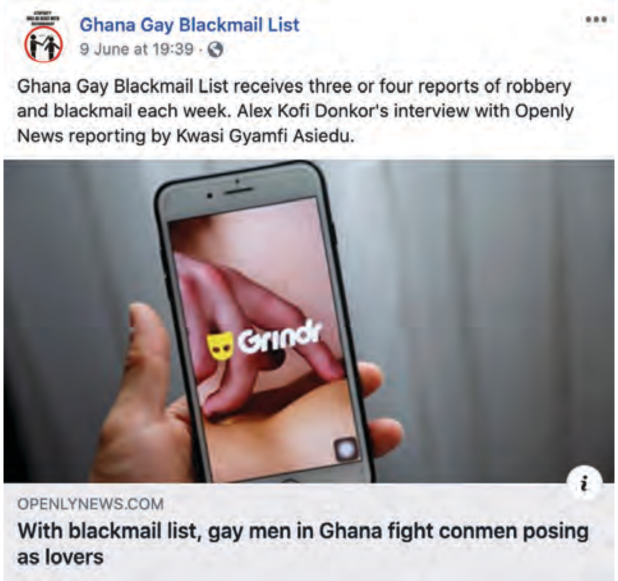
In Morocco, photos of men taken from gay social apps, such as Grindr, Hornet, and PlanetRomeo, were circulated online after a Moroccan transgender model and social media influencer living in Turkey told her Instagram followers in April 2020 to create fake accounts on gay dating apps to find out how common homosexuality is within Morocco, a country where same-sex sexual acts are illegal. Social apps like Grindr will show other users who are geographically closest to you first, even if users have disabled the distance setting and haven't uploaded images to their profiles, meaning that family members and neighbours were likely outed during the COVID-19 lockdown. Those that did have images on their profiles had their photos circulating online.

The total number of people outed was reported to be between 50 and 100, with Moroccan LGBTQIA+ charities reporting an increase in reports of homophobic abuse and requests for support. Victims of abuse are unlikely to go to the police because same-sex sexual acts are illegal under Article 489 of the Moroccan criminal code and past encounters between the LGBTQIA+ community and Moroccan law enforcement have been deplorable, including for the transgender community. As a result of this digital "outing" campaign, one person committed suicide out of desperation, at least three men were kicked out of their homes, and others were left fearing for their lives.

An unfortunate common theme across the globe is the use of social media and dating apps by criminals to target members of the LGBTQIA+ community and cause them harm or steal from them, and Africa is no exception to this theme.

In South Africa, which has legal protections and recognition of LGBTQIA+ individuals in place, there are reports that criminals have used social apps as a way to surveil a victim's home security systems and valuable items before later committing burglary, or even luring a victim into meeting and then kidnapping, threatening, stripping, and ultimately stealing from them. In Ghana, where same-sex sexual acts are illegal, criminals are also using social apps to identify, lure, blackmail, and steal from LGBTQIA+ individuals, with some incidents being purely homophobic in nature. Similar incidents occur in Nigeria, with 70 recorded incidents of blackmail/extortion being used against the LGBTQIA+ community in 2018, many of which were premeditated and set up through social apps like Grindr, Badoo, and ManJam.

The significant difference between the incidents in South Africa, versus Ghana and Nigeria, is that criminals can more effectively use outing the individual as an extortion technique in Ghana and Nigeria because being outed could result in up to three years in prison in Ghana, or the death penalty in Nigeria. Whereas victims in South Africa can report incidents and criminals to the police, victims in Ghana and Nigeria would become criminals by doing so. For example, a Nollywood filmmaker named After Obed was beaten and robbed after being lured into a meeting with a criminal through Grindr, and was arrested alongside his attackers and spent a few days in jail before paying $555 for his release. The LGBTQIA+ communities in Ghana and Nigeria are bravely fighting back; activists in Ghana created a 'Ghana Gay Blackmail List' to expose criminals targeting gay men, whilst LGBTQIA+ Nigerians created a website called 'Kito Diaries' to share their stories, warn others, and name attackers.



Ghana Gay Blackmail List
9 June at 19:39 ·

Ghana Gay Blackmail List receives three or four reports of robbery and blackmail each week. Alex Kofi Donkor's interview with Openly News reporting by Kwasi Gyamfi Asiedu.

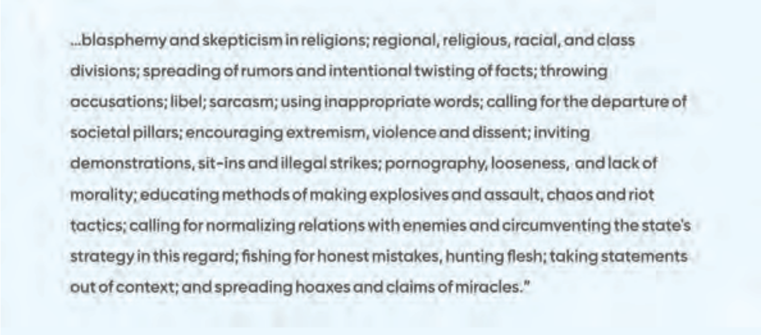
OPENLYNEWS.COM
With blackmail list, gay men in Ghana fight conmen posing as lovers

A Facebook post on the Ghana Gay Blackmail List page.

Surveillance

There are reports that Egyptian security forces were already surveilling the LGBTQIA+ community on a broader scale prior to the concert in Cairo in September 2017, which may have contributed to the number of LGBTQIA+ people being arrested quadrupling under President al-Sisi. Earlier in 2017, a lawyer named Mohamed Bakeer claimed that the Egyptian security forces were surveilling the LGBTQIA+ community by searching for Egyptian profiles on international dating websites, creating fake accounts, and arranging meetings with LGBTQIA+ individuals to entrap and arrest them, in addition to using contact details to tap mobiles, wire apartments and setup string operations.

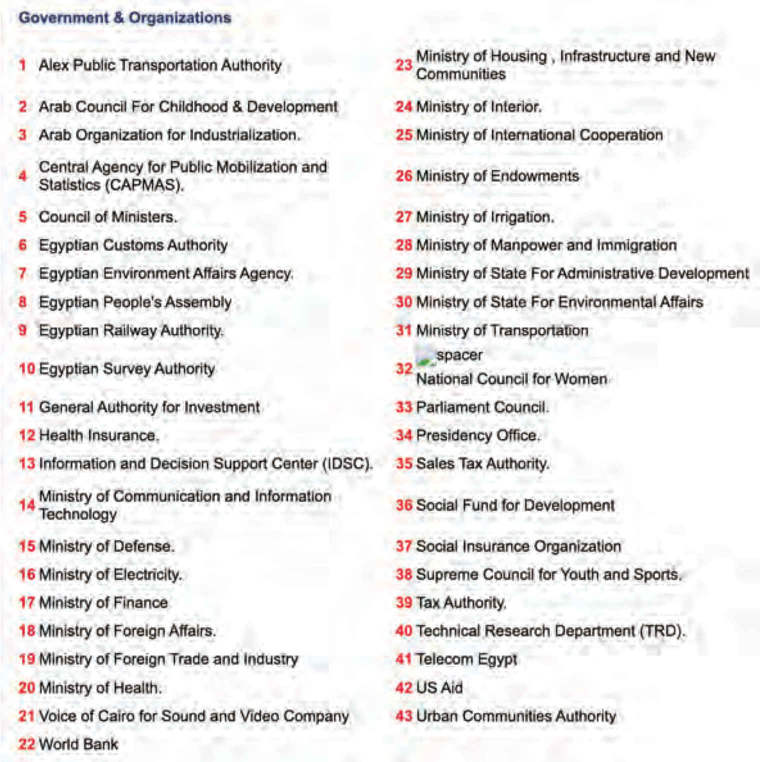
A proposal from Egypt's Interior Ministry was leaked in 2014, showing that they were looking to implement a system to scan social media sites and mobile apps like Facebook, YouTube, and other social networks such as WhatsApp to identify "destructive ideas" such as "pornography, looseness, and lack of morality" that could pose a threat to Egyptian society, and search for "keywords that constitute a violation of the law and public moral [sic], or that do not fit into norms and societal ties." This almost certainly includes the targeting of LGBTQIA+ individuals given that they are regularly arrested under a 1960s anti-prostitution law prohibiting immorality and debauchery. The proposal also sought the ability to create an unlimited number of accounts to infiltrate and interfere with groups.



...blasphemy and skepticism in religions; regional, religious, racial, and class divisions; spreading of rumors and intentional twisting of facts; throwing accusations; libel; sarcasm; using inappropriate words; calling for the departure of societal pillars; encouraging extremism, violence and dissent; inviting demonstrations, sit-ins and illegal strikes; pornography, looseness, and lack of morality; educating methods of making explosives and assault, chaos and riot tactics; calling for normalizing relations with enemies and circumventing the state's strategy in this regard; fishing for honest mistakes, hunting flesh; taking statements out of context; and spreading hoaxes and claims of miracles."

The Interior Ministry's examples of 'destructive ideas.' Source: Privacy International.

Buzzfeed reported in September 2017 that "several anonymous Egyptian government officials" confirmed that a company called "See Egypt" won the contract and had begun monitoring Egypt's online communications. See Egypt is a sister company of the American company "Blue Coat," which allegedly sold similar technology to the Syrian regime in 2011, and Blue Coat's monitoring devices were also detected in Iran and Sudan in 2013. Following Buzzfeed's report, Egypt's Interior Ministry denied they had contracted See Egypt for online communications monitoring. However, See Egypt's own website today confirms that the Ministry of Interior is a customer, and the list of other governmental customers confirms See Egypt's strong ties with the Egyptian government.



Government & Organizations

1 Alex Public Transportation Authority
2 Arab Council For Childhood & Development
3 Arab Organization for Industrialization.
4 Central Agency for Public Mobilization and Statistics (CAPMAS).
5 Council of Ministers.
6 Egyptian Customs Authority
7 Egyptian Environment Affairs Agency.
8 Egyptian People's Assembly
9 Egyptian Railway Authority.
10 Egyptian Survey Authority
11 General Authority for Investment
12 Health Insurance.
13 Information and Decision Support Center (IDSC).
14 Ministry of Communication and Information Technology
15 Ministry of Defense.
16 Ministry of Electricity.
17 Ministry of Finance
18 Ministry of Foreign Affairs.
19 Ministry of Foreign Trade and Industry
20 Ministry of Health.
21 Voice of Cairo for Sound and Video Company
22 World Bank
23 Ministry of Housing , Infrastructure and New Communities
24 Ministry of Interior.
25 Ministry of International Cooperation
26 Ministry of Endowments
27 Ministry of Irrigation.
28 Ministry of Manpower and Immigration
29 Ministry of State For Administrative Development
30 Ministry of State For Environmental Affairs
31 Ministry of Transportation
32 spacer National Council for Women
33 Parliament Council.
34 Presidency Office.
35 Sales Tax Authority.
36 Social Fund for Development
37 Social Insurance Organization
38 Supreme Council for Youth and Sports.
39 Tax Authority.
40 Technical Research Department (TRD).
41 Telecom Egypt
42 US Aid
43 Urban Communities Authority

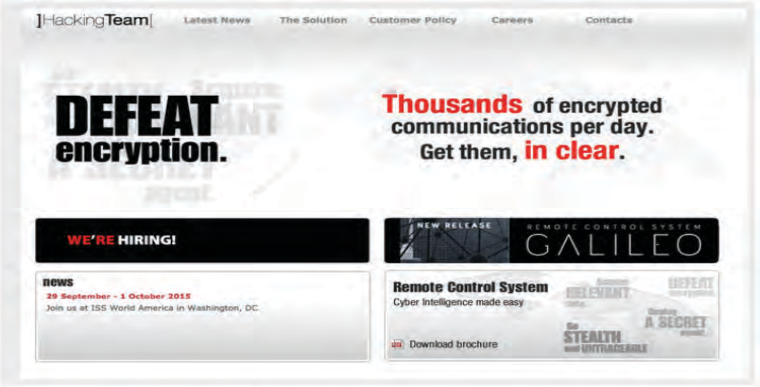
See Egypt's 'Government & Organizations' customers (Source: See Egypt)

See Egypt's solution also enables the Interior Ministry to use Deep Packet Inspection (DPI) technology. DPI is an advanced form of examining and managing network traffic that can easily identify the senders or recipients of communications and can be used to eavesdrop, monitor and take actions on network traffic, for example re-routing, censoring or blocking communications. See Egypt's CEO told Buzzfeed that See Egypt would give the Interior Ministry the system, train them to use it, and show them how to comb through the data gathered from various sources like email, social media, messaging apps like Whatsapp and other programs.

Most worryingly, an anonymous Interior Ministry official informed Buzzfeed that they were using the solution for a broad mandate, including monitoring communities that the Egyptian government considers a risk including those engaged in "debauchery" or "homosexual acts," and that "dozens of Facebook groups" used by the LGBTQIA+ community were being watched. The capabilities of See Egypt's solution are consistent with some of the methods used by Egypt's security forces during the crackdown in September 2017, such as arresting an individual who posted positively about the concert in Cairo on Facebook, creating a fake LGBTQIA+ community Facebook page, and identifying other members of the LGBTQIA+ community.

The LGBTQIA+ community in Uganda fell victim to a phishing campaign in early 2014 that an NGO called "Unwanted Witness" soon identified to be related to Zeus malware, just two months after a controversial anti-homosexuality law was enacted. Zeus is a Windows-based spyware that can be used to steal information from the victim's machine through man-in-the-browser keystroke logging and form grabbing, and is often spread through drive-by downloads and phishing campaigns. Unwanted Witness reported that Zeus stole the mailing lists of victims and used that information to further spread the malware amongst the LGBTQ+ community.

Leaked emails in 2015 between an Israeli surveillance company called NICE Systems and an Italian surveillance company called Hacking Team described an upcoming business opportunity of selling surveillance software to the Ugandan government, having already sold surveillance software to Uganda's police force. The leaked emails show the Hacking Team explaining how they use malware and vulnerabilities to infiltrate computers and smartphones for monitoring purposes. An email chain from July 2012 shows NICE Systems and Hacking Team discussing a security article regarding a malware specimen being analyzed and they express relief that the malware in question was being linked to cybercriminals and, after being described as a potential new Zeus malware, a Senior Security Engineer at Hacking Team writes, "Anyway as long as they think we're the new zeus [sic]." One source identified the malware as being sold by the Hacking Team, and in the leaked emails a Hacking Team employee wrote "In any case, those who identified us as the hacking team are dr webb (who also calls us criminals), but they seem to have had a cue. None of the other big names have understood what it is."



news

29 September - 1 October 2015

Join us at ISS World America in Washington, DC

Hacking Team's website as of Aug. 24

Hacking Team

Hacking Team's website as of 24th August 2015 (Source: Buzzfeed)

Without having a specimen of the malware used in the phishing campaign against the Ugandan LGBTQIA+ community in 2014, it is not possible to determine whether it was indeed Zeus malware or if it could have been spyware created by Hacking Team and sold to Uganda's police force and then used to monitor the LGBTQIA+ community. Recorded Future has reached out to Unwanted Witness to try to obtain an original specimen of the malware used in the phishing campaign against the LGBTQIA+ community in Uganda.

Censorship

Following the concert crackdown on the LGBTQIA+ community in Egypt, the Supreme Council for Media Regulation (SCMR) banned any media outlets from supporting the LGBTQIA+ community and ordered that the only acceptable content would be remorse or admitting that being homosexual is unacceptable. The ban was implemented after the head of the SCMR, who was directly appointed by President al-Sisi, stated that homosexuality was a "shameful disease" and shouldn't be promoted, which is just one instance of the SCMR censoring media based on moral issues.

In May 2017, Kenya's Film Classification Board (KFCB) announced that they would collaborate with Kenya's Cybercrime Police Unit, the Directorate of Criminal Investigations, and service providers like Google to crack down on online platforms promoting illegal activities including "spreading vices such as homosexuality." The KFCB have previously banned or attempted to ban LGBTQIA+ media including movies and music videos like "Rafiki," a movie about two women who fall in love in Kenya, and Macklemore's "Same Love" music video, claiming that homosexuality is being imposed on Africa. A similar stance is taken by other African countries where same-sex sexual acts are illegal. For example, Uganda's censorship board banned a Dutch film called "The Dinner Club" for "glorifying homosexuality." Even South Africa, where there are protections for LGBTQIA+ persons, has banned LGBTQIA+ movies and could be helping in the censorship of LGBTQIA+ content in Kenya. The continued censorship of LGBTQIA+ media throughout Africa reiterates the myth that homosexuality is a "Western import" and "un-African."

Recommendations

Threat actors will continue to target marginalized individuals and communities, so we want to empower members of the LGBTQIA+ community to take their rights to privacy and security into their own hands wherever possible. Based on findings across the breadth of topics previously discussed, Insikt Group recommends the following actionable steps for the LGBTQIA+ community:

- Become familiar with apps' privacy policies (data retention periods, third-party data sharing) before providing personal information. Users should be especially aware of how apps handle location information, if applicable, and be wary of any apps that are not transparent about these policies.
- As mentioned in the earlier App Study section, some social apps have implemented, or are in the process of adding, features to warn LGBTQIA+ users when they are using the app in a country with discriminatory laws. Likewise, members of the LGBTQIA+ community should arm themselves with information about potential stigmatization and discriminatory laws in any unfamiliar travel destinations.
- Be vigilant in securing all accounts for online communities. Most criminal and underground threat activity that targeted apps popular in the LGBTQIA+ community over the past year was related to credential theft or sales. Combat this by using long, complex passwords and multi-factor authentication wherever possible. Do not use the same password across multiple accounts, and change passwords periodically. Password managers such as LastPass can help facilitate all of these tasks.
- Exercise caution when arranging to meet with individuals from LGBTQIA+ dating apps in countries with anti-LGBTQIA+ laws by taking steps to confirm the identity of the person, arranging to meet in a public place, and informing a trusted contact to mitigate the threat of law enforcement or criminal entrapment.
- A virtual private network (VPN) can be used to increase security and to evade state supported surveillance; however, such networks need to be employed with care as some nations have moved to actively ban their use.

Outlook

Further data exposures from social and dating apps popular with the LGBTQIA+ community, such as those that affected Grindr and Jack'd, are likely. These apps will almost certainly continue to share data with third parties and only user pressure, or a substantial fine for breaching data privacy laws, is likely to make these apps reconsider. Users should exercise caution when deciding which social and dating apps to use, and should pay particular attention to the apps that do not obfuscate geolocation data in countries with a poor stance on LGBTQIA+ rights.

Compromised account credentials and user data from social and dating apps will continue to be posted on dark web and underground sources. This offers an extortion opportunity for cybercriminals who could purchase leaked credentials to obtain intimate personal details and/or photos of individuals. Users should follow the recommendations laid out on the previous page to mitigate the threat of credential abuse.

States will continue to target, surveil, and censor the LGBTQIA+ community for as long as they view the community as an external threat to security, society, or morality. States will continue to employ techniques such as law enforcement entrapment through social and dating apps, large-scale surveillance through DPI technology and infiltration of the community, and censorship of LGBTQIA+ content to deny the legitimacy of the community. State discrimination against the community emboldens criminals who will continue to target, entrap, extort, harass, and otherwise harm LGBTQIA+ individuals. Criminalizing the community will continue to encourage criminal acts against the community.

About Recorded Future

Recorded Future delivers the world’s most technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. Recorded Future’s proactive and predictive platform provides elite, context-rich, actionable intelligence in real time that’s intuitive and ready for integration across the security ecosystem. Learn more at recordedfuture.com.