UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

December 2012

2012 CyberWatch Year in Review:

Middle East and North Africa, Southeast Asia,

Latin America and the Caribbean

TABLE OF CONTENTS

INTRODUCTION

The Citizen Lab's CyberWatch publications monitor trends and developments on the intersection of information communications technologies (ICTs), global security, and human rights in three regions — Middle East and North Africa, Southeast Asia, and Latin America and the Caribbean. Our assessment of events that took place in 2012 has found that freedom of expression continues to be under threat in these parts of the world, although some progress has been made in certain countries. This review discusses trends in cyber

attacks, changing legal norms, social media use, technological development, censorship and filtering, and arrests of rights activists.

CYBER ATTACKS

Technological development and laws of countries in the Southeast Asian region have not kept pace with the increased use of computers in the public and private sector. As a result, these institutions often find themselves vulnerable to attack. In a report titled the Cyberthreat Forecast for 2012 [PDF], Kaspersky Labs stated that it is likely that there will be more incidents of cyber crime and attacks in Southeast Asia as online and mobile services in the region continue to expand.

Malaysia's Ministry of Science, Technology, and Innovation, which serves as the national centre for monitoring and preventing online crime, reported that the number of cyber crimes in 2011 is nearly double that of 2010. In June 2012, Defense Minister Ahmad Zahid Hamidi urged the Association of Southeast Asian Nation (ASEAN) to develop a "master plan" to counter cyber attacks. The government of Japan has said that it will create a "cyber defense network" with ASEAN by facilitating contact "between officials in charge of cyber attacks in each country so they can share information about attacks."

The Philippines has faced a number of cyber attacks in protest of the controversial Cybercrime Prevention Act. The bill was heavily criticized for, among other things, its ambiguous definition of online libel and harsh legal punishments for Internet defamation. After the Act was passed, a group calling themselves PrivateX hacked seven government websites. This was followed by a spate of defacement attacks in September and October by Anonymous Philippines. The Supreme Court subsequently issued a 120-day temporary restraining order (TRO) against the Act's implementation after lawyers and media organizations filed 15 petitions seeking to declare as unconstitutional the whole or portions of the legislation. In early December, the government asked the Supreme Court to lift the TRO as it maintained the legality of the law and rejected accusations that it is trying to regulate or punish free speech.

Following reports in June that the US and Israel jointly developed Flame—a piece of malware used for cyber espionage—Iran's then Minister of Information and Communications Reza Taqipour made a formal complaint [Farsi] about foreign government-sponsored cyber attacks, although Iranian officials contended that the virus caused no noticeable damage [Farsi]. Iran has reportedly taken significant steps toward improving its defense capabilities against malware attacks, which were said to number [Farsi] 500 a day on average. The Ministry of Information and Communications Technology strongly urged [Farsi] government organizations to prepare themselves for potential Internet-based attacks, while the armed forces [Farsi] took similar defensive measures. To that end, Iran and North Korea have reportedly signed a mutual protection treaty against Western malware attacks.

A new virus called MiniFlame was discovered [Farsi] in July, though Kaspersky Lab later asserted [Farsi] that it is an "independent module" rather than a component of Flame. In October, the US accused Iran of a series of cyber attacks against Western financial institutions and Gulf energy companies, including Saudi Aramco

and RasGas, a Qatar-based natural gas producer. These attacks coincided with US Defense Secretary Leon Panetta's warning that the US faces the possibility of a "cyber Pearl Harbor" attack against its critical infrastructure and thus need to bolster its defenses. The Iran Revolutionary Guard Corps [Farsi] and MICT [Farsi] have both denied any involvement in the attacks.

The ongoing civil war in Syria spilled into cyberspace with pro-government actors and sympathisers of the Syrian opposition directing malware attacks and misinformation campaigns against each other. In June, TIME Magazine reported that the US government was providing Syrian rebels with "logistics aid" and training in "communication security", including PC encryption and secure cellular phone use. In that same month, the Citizen Lab and Electronic Frontier Foundation (EFF) uncovered a trojan targeted at Syrian dissidents called BlackShades Remote Controller, which was distributed as a ".pif" file over Skype. EFF has since uncovered more malware attacks against Syrian dissidents and activists, including a fake anti-hacking tool and fake PDF files, both of which install DarkComet Remote Administration Tools (RAT), which provide the ability to remotely survey the electronic activities of a victim by keylogging, remote desktop viewing, webcam spying, audio-eavesdropping, data exfiltration, and more.

Pro-government hackers, many of whom claiming to be members of the Syrian Electronic Army (SEA), compromised and defaced a number of social media platforms and popular news websites over several months. In July, for instance, the SEA hacked the Twitter and Facebook accounts of Al Jazeera's The Stream program. A series of similar attacks against international news media followed as pro-government actors compromised Amnesty International, Reuters, and Al Jazeera's SMS service and front page. The hacker collective Anonymous, which has also taken action against the Yemeni and Emirati governments, responded by taking down the SEA's website and allegedly leaking thousands of Syrian government documents to WikiLeaks. Assad's regime itself has been accused of jamming BBC services to the Middle East and cutting the Internet off entirely to the Syrian population.

In Latin America, sophisticated forms of phishing have become a widespread problem for bank customers. Online banking users across the region have received convincing emails claiming to be from their banks, asking for private information or instructing users to change their passwords. These phishing scams have taken up to tens of thousands of dollars from individual user's accounts. Total losses for banks in the region add up to approximately 90 billion dollars in the past year. Major banks such as Banco BMG, Banco Bradesco, and many others have also been targeted by DDoS attacks, with Anonymous Brasil admitting participation. The number of DDoS attacks in Latin America have gone up in the past few years.

The increase in social media use by government officials and public figures has made hacking of their accounts an issue. Hackers compromised the Twitter account of the President of Venezuela's National Assembly this past September and tweeted a series of fake messages claiming that a violent coup was taking place. Additionally, people who have been critical of the Chavez government have been victims of hacking, with pro-Chavez messages being sent from their accounts. Recently, the pro-government group N33 has admitted their involvement in these attacks. Despite hacking being illegal in Venezuela, investigations into these attacks have not resulted in action.

LEGAL MECHANISMS

A number of countries have used legal mechanisms to control online content in various ways. Not all of these legal instruments were drafted to regulate freedom of speech, though this has been disputed by activists in many cases.

In Southeast Asia, the leaders of the 10 member states of the regional bloc signed the ASEAN Human Rights Declaration (AHRD). The declaration has been heavily criticized by human rights groups not only because the drafting process lacked transparency, but also because it contains caveats to the protection of human rights. For example, the AHRD includes a guarantee on freedom of opinion and expression through Article 23. However, the framework for free speech is further narrowed by Article 21, which states that "Every person has the right to be free from … attacks upon that person's honour and reputation." Those phrases can be used by governments as a tool for legitimation when jailing critics.

The fear of cyber crime has prompted a number of countries to expand existing laws or draft new ones. The Philippines, for example, enacted the controversial Cybercrime Prevention Act to "increase privacy protection and deter Internet fraud and identity theft" amongst a great range of other online threats. Vietnam has prepared two draft decrees that make foreign commercial entities responsible for providing user data to the government on demand, and mandate that those companies locate at least one server and one representative in Vietnam. Malaysia has announced that it will repeal the 1948 Sedition Act, which was originally introduced by the British colonial government to suppress Communist elements, but more recently been used by the ruling Barisan Nasional coalition to shut down government criticism. In its place, the government plans to introduce the National Harmony Act, which is supposed to "safeguard the right to freedom of speech while protecting national unity by preventing the incitement of religious or ethnic hatred." Human rights activists have held out full endorsement of the new act until details are known. Malaysia's 1950 Evidence Act remains in effect, with concerns raised that recent amendments may make citizens unjustly liable for content posted online and leading some blogs and prominent Malaysian websites to protest the revisions through a temporary blackout. Similarly, Thailand's criminal code provision on lèse majesté and the Computer Crimes Act continue to be used extensively to punish foreigners, members of the Red Shirts movement, and activists for posting online comments deemed insulting to the monarchy. Despite calls for reform, Thai legal authorities recently upheld lèse-majesté laws as constitutional.

Following the Arab Spring, the Middle East and North African region continues its uphill struggle for democracy. Several countries have enacted new pieces of legislation that mandate parameters for what can be communicated, offline and online, as others continue to work toward greater freedom. Both the United Arab Emirates and Qatar have respectively revised existing cyber crimes laws and drafted new laws to penalize criticism of government figures and the monarchy, similar to lèse-majesté laws in Thailand. This is in contrast to Tunisia where state-sanctioned censorship has ended. Efforts to introduce online controls in Jordan have been marked by a backlash from local civil society. The proposed amendments to the 1998 Press and Publications Law, which would make website owners criminally liable for content and order them to register with local press associations, have resulted in a civil movement towards greater Internet freedom, akin to the reaction seen in the Philippines against that country's proposed cyber crimes law.

Iran, the fourth most censored country according to CPJ's 2012 report, has restructured its surveillance system by adding a new Supreme Council of Cyberspace (SCC). The SCC was created following a direct order [Farsi] from the Supreme Leader to have "constant and comprehensive monitoring over the domestic and international cyberspace." The council's task is to supervise all entities [Farsi] involved in cyber security, including the Passive Defense Organization and the cyber departments of the Islamic Revolution Guards Corps and the Ministry of Intelligence and National Security. The council would also administer Internet and mobile networks, as well as manage large-scale infrastructure projects, such as the creation of a national Internet.

In Latin America and the Caribbean, a number of governments have proposed bills intended to criminalize various types of cyber crimes, including file sharing and violations of privacy. However, many of these bills have been criticized by civil society groups for being too restrictive. In Panama, for instance, protests erupted after Bill 510 — On Copyright and Related Rights — was passed. As a consequence, President Ricardo Martinelli vetoed part of the bill that would allow heavy fines on those accused of copyright infringement. A similar situation happened in Costa Rica, in which the cyber crime bill Ley 9048 incited protest from the media community for restricting what journalists are allowed to say online. The bill was eventually amended so as not to incriminate journalists.

Argentina's Audiovisual Communication Services Law proposed by President Cristina Kirchner's government was one of the issues that precipitated mass protests in November. The law sought to break up Grupo Clarín, the largest media network in Argentina, by removing many of its licenses. The government stated that it aimed to limit the number of media stations a company can own and therefore make communications technology cheaper and more democratic. However, many members of the Argentine press have interpreted this effort as a means to impose limitations on Grupo Clarin, which has been highly critical of the Kirchner government.

Civil society played a key role in the drafting of Brazil's Marco Civil da Internet (otherwise known as the world's first Internet bill of rights), which aimed to protect online user rights and free speech. Groups such as Article 19, Access, and Association for Progressive Communications came out in support of the bill. However, the vote to pass the bill was postponed five times in parliament and it was finally shelved indefinitely in November.

SOCIAL MEDIA USE

The increasing number of social media users worldwide and the Arab Spring are causes for concern for those who are worried that technological advances might be used for political purposes. As a result, governments have taken significant steps over the past year toward controlling information flows over social networking platforms like Facebook and Twitter, as well as blogs. Some countries have even released new legislation that specifically targets social media.

As Myanmar undergoes a political transition, the country released a new telecommunications bill that could potentially prohibit social media and "unregistered gadgets," as well as permit the government to intercept data transmissions and suspend telecommunications services. Social media has provided a platform for Singaporeans to criticize their government openly. In July, the government of Singapore, which has called for the establishment of an Internet code of conduct to "encourage civilized behaviour", set up the Media Literary Council to "spearhead public education on media literacy and cyber wellness". Netizens had said "no" to the code due to concerns that it would provide a mechanism to restrict free speech online and will remain vigilant against attempts by the council to regulate the Internet. In Thailand, Maj Gen Bunjerd Tientongdee, the deputy director of the Department of Defence Information and Space Technology within the Ministry of Defense, stated that the military is concerned that the widespread use of social media "could lead to public misinformation" and increase the risk of cyber attack. As such, it is working with other ASEAN countries to develop an integrated cyber security policy.

In August, a Bahraini parliamentary bloc developed a "code of honour" to govern social media content and ensure that users do not "divide the society" or spread sectarianism. A month later, the Bahraini Ministry of Interior announced its intention to prosecute those who engage in "defamation and abuse" on social media platforms. Social media use in Bahrain has skyrocketed over the past year: 51 percent of the country's 900,000 Internet users now use social networking websites, including 340,000 on Facebook and 60,000 on Twitter. Kuwait has similarly proposed passing legislation that criminalizes the "misuse of social media."

Other countries have employed coercion to control social media. In September, Vietnamese authorities cracked down on three popular dissident blogs, arresting their administrators and ordering public employees not to access them. The government accused the websites of "publishing distorted and fabricated articles against the leadership", a violation of Article 88 of the Criminal Code. The Arabic Network for Human Rights Information has similarly criticized Oman for taking harsh measures against activists and bloggers.

Nevertheless, citizens have continued to use social media as a vehicle for mobilization and organization of opposition. In Kuwait, anonymous Twitter users called for two mass mobilizations in response to changes to the country's electoral law. The October protests were the largest in the nation's history and Kuwaitis took to the streets again in November. Around the same time, several Mauritanian bloggers launched a campaign with the aim of criticizing foreign mining corporations for numerous rights violations. The bloggers took to Twitter and Facebook, using the hashtag "#ضد_نهب_معادن_نا" ("against_mining our minerals"). Similarly in Argentina, mass anti-government protests that occurred in November against President Kirchner's government were organized primarily on social media, with netizens using the hashtag #8N on Twitter and pages such as "El Anti-K" on Facebook, to discuss their views on the protest.

Social media played a key role in electoral processes in Indonesia and Malaysia. Candidates for the 2012 Jakarta gubernatorial election used Skype, YouTube, and browser-based computer games to sway voters. Over 500,000 tweets about the two main candidates—incumbent Fauzi Bowo and former Surakarta Mayor Joko Widodo—were generated between July and August alone. In Malaysia, social media as a political tool was embraced early by the opposition — the Pakatan Rakyat coalition — in the 2008 election and resulted in the ruling Barisan Nasional coalition losing its grip on majority in parliament for the first time since the country's

independence. Ahead of the 2013 election, Barisan Nasional's Youth Chairman Khairy Jamaluddin has urged the government to "use social media to its advantage".

In Iran, election campaigns got an early start on Facebook. With a couple of months until the start of the presidential election cycle, a number of prospective candidates such as Mohsen Rezaei [Farsi], Mohammad-Bagher Ghalibaf [Farsi], and Saeed Jalili [Farsi] have started building an online presence. Esfandiar Rahim Mashaei, a close confidant of Mahmoud Ahmadinejad, is also one of the potential candidates for the upcoming presidential election. His campaign has generated several Facebook pages in an attempt to connect with a larger group of fans. It seems [Farsi] that Mashaei's team plans to use social media as a tool to garner support despite restrictions on social networks within Iran.

A number of countries have also used social media for crisis mapping and to reveal the abuse of power. The Tunisian Association for Digital Liberties created Yezzi, a website that collects "violence testimonies sent by mobile, web, email, and SMS" and then map their locations with the aim of exposing police abuses and engendering accountability. Around the same time, a group of Egyptian youth built a website called the Morsi Meter to monitor the performance of the Egyptian president and hold him accountable to his campaign promises — as of December 2012, he has fulfilled only 10 out of 64 promises. Saudi Arabian activists in the country's Eastern Provinces documented abuses by security forces by posting videos of violent clashes, while in Indonesia, a YouTube video showing the torture of civilians in the restive region of Papua resulted in the jailing of three Indonesian soldiers.

Military branches have also engaged directly with social media. The Israel Defense Forces (IDF) and Hamas' al-Qassam Brigades, have treated social media as platforms for disseminating propaganda and conducting psychological operations. On November 4, the IDF announced the commencement of military operations against Hamas via Twitter. An exchange of propaganda, threats, and live updates between the two sides ensued over Twitter, Facebook, and YouTube.

In the Caribbean, social media has been used as a citizen-led emergency response tool. When Hurricane Sandy hit the region and disrupted many lines of communication, bloggers from Cuba, Jamaica, Haiti, and the Bahamas posted updates of the destruction online. Twitter was also a popular tool used for reporting on the storm. When Cuba was hit by a massive blackout early in September, government and media outlets had remained silent for the first few hours, offering no information to millions of citizens. However, Cubans began communicating through Twitter using the hashtag #Apoganzo (meaning "blackout" and "strike") to bring updates to citizens from all over the affected region.

In the Middle East, women's rights issues have surfaced on social media regarding the headscarf (otherwise known as the "hijab"). In Iran, a group called the Iranian Liberal Students and Graduates launched [Farsi] a "No to Mandatory Hijab" campaign on Facebook to emphasize freedom of attire. Since July, the campaign has gathered over 30,000 'likes' and dozens of Iranians, men and women, have expressed their opposition to the mandatory hijab. Controversy around a similar campaign arose in November, when Facebook censored pictures of a Syrian woman with her hair uncovered while holding a passport containing a photo of herself

wearing a headscarf in a group called "The uprising of women in the Arab world." Facebook maintained that this was because users reported the material as "offensive and insulting".

In Indonesia, Facebook has increasingly been used by kidnappers for sex trafficking purposes. As of October, 27 missing Indonesian children are believed to have been abducted after meeting their captors on Facebook. That number has already surpassed the 18 comparable cases reported for all of 2011.

TECHNOLOGY

In 2011, Iran announced that it seeks to establish a national Internet, which would conform to [Farsi] the regime's "religious and revolutionary values". Although they have been working on this project since 2002, President Mahmoud Ahmadinejad's administration recently stepped up the process as pro-democracy protests spread rapidly across the region and a number of cyber attacks hit its nuclear installations. Also referred to as the "Pure" or "Halal" Internet, the National Information Network is the biggest project of its kind in the region, with an approximate budget of US$1 billion. This network is intended to be uncensored and supposed to act as "defence mechanism" against cyber attacks, as well as providing a faster and more reliable connection for users. Criticism has been leveled against the network as it could be used as a tool to monitor user activities and to disconnect Iranian cyberspace from the rest of the world. Moreover, the government has mandated for all government websites to be hosted on Iranian servers and has launched a number of domestic products, including a search engine, an operating system, e-mail services, anti-virus programs, and software products. Mehr, a video sharing site described as a "sanitized alternative to YouTube", was launched in early December. The service is maintained by the state-run Islamic Republic of Iran Broadcasting.

Due to growing pressure and economic sanctions from the US and other Western countries, Syria has turned to China for its telecommunications needs. The Syrian Telecommunications Establishment (STE) has cemented business ties with Chinese companies for Internet bandwidth. Renesys reported in August that PCCW, a Hong Kong-based company, was "carrying the lion's share of Internet traffic into Syria." Elsewhere in the Middle East, the Libyan government has reportedly re-deployed interception and surveillance equipment once used by former dictator Muammar Qadhafi. It is supposedly being used to track communication between remaining Qadhafi loyalists.

In Southeast Asia, Myanmar has begun to reform its telecommunications sector. The country unblocked some 30,000 websites in September 2011, allowing citizens to access unofficial political content for the first time in years. The Ministry of Communication is now encouraging foreign investment in its telecommunications sector, drafting a new media law, and trying to "increase mobile penetration by 50 percent by 2015." Currently, less than one percent of Myanmar's population has access to the Internet. In contrast, the neighbouring country of Vietnam has the third highest Internet penetration rate in the region behind Indonesia and the Philippines.

The rise in Internet use throughout Latin America and the Caribbean has resulted in growing investment in technology. Due to the growth in cloud storage, streaming, and other Internet services, Chile was chosen to be

the site of Google's first South American data centre. The search engine giant will invest US$150 million to build a mid-sized centre. As part of its Community Access Points program, the Jamaican government has announced plans to expand access to Internet services to thousands across the country by the end of 2012. This initiative will make the Internet accessible in public community areas.

CENSORSHIP AND FILTERING

Censorship in the name of combating pornography is increasing. In September, Hamas announced plans to censor pornographic sites in the Gaza Strip, making ISPs responsible for their filtration. In Egypt, the Prosecutor General ordered government ministries to enforce a 2009 court decision to ban pornographic sites. While these decisions have been "top-down", a grass-roots anti-pornography campaign in Jordan gained momentum this year, leading the Jordanian government to offer anti-pornography software to families on demand. In Oman, a group of citizens drafted an "Omani Ethics Code for Electronic Publishing", which the group hoped would help Internet users avoid putting content in cyberspace that may be lead to further crackdowns against the online community. While well-intentioned, the code can also be seen as evidence of a climate of self-censorship that Oman's online community feels is necessary to avoid government persecution.

After receiving reportedly "millions of complaints" on the proliferation of Internet pornography, the Indonesian Communications and Information Ministry announced that they would discuss with Google and YouTube means of blocking pornographic sites. In addition, Nawala Nusantara, an Indonesian filtering service, announced a partnership with the Association of Indonesia Internet Service Provider (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)) to provide filtering services on APJII-owned servers.

Research performed by the Citizen Lab relating to censorship in Oman has yielded interesting insights into how filtering in one country can inadvertently affect content controls in another, otherwise known as "upstream filtering". As Omani telecommunications companies have peering agreements with Indian ISPs, testing has indicated that content censored in India that would otherwise be freely accessible in Oman is also censored, with Indian notification of blocked pages appearing when access in Oman is attempted.

Some countries in the Middle East and North Africa have moved toward greater Internet freedom. Tunisia and Libya have been noted by Freedom House in their annual report [PDF] as having a significantly higher Internet freedom rating in 2012 compared to 2011. The same report, however, indicated that Syria and Iran were the "least free" countries in the region with regards to online rights. Syria has escalated its censorship to by cutting itself off from the Internet entirely. The government claimed that it was due to technical problems, but the incident was seen by the international community as a way of blocking reports on the current conflict.

In Iran, filtering has been used as a political tool by the government's more conservative faction. Several pro-Ahmadinejad weblogs were filtered [Farsi] by the country's judiciary due to comments critical of the Chairman of Parliament Ali Larijani. Larijani is known as one of the main critics of Ahmadinejad's

government, who is also fully supported by Ayatollah Khamenei. Additionally, a number of weblogs known to be critical of Ahmadinejad and his government have also been filtered.

Content considered to be blasphemous to Islam has been targeted for filtering in several countries. In response to the Innocence of Muslims video, Saudi Arabia called for the creation of a global Internet censorship body that would be in charge with overseeing cyber crime as well as dealing with what it sees as inappropriate content on websites. In addition, the Saudi government has proposed a new law imposing penalties on users who post blasphemous content on social media sites. The Innocence of Muslims controversy has also resulted in more drastic means to filter content in Iran. The Iranian government filtered Google and Gmail as unintended consequences of attempting to block the secure-protocol version of YouTube. Iranian officials publicly announced that they did not have plans to block access to Google services and unblocked Gmail due to intense public pressure. This incident shows that there are limits to what the authorities can do without facing a major backlash. Access to the Innocence of Muslims video was blocked in Singapore, Malaysia, and Indonesia after requests were made by those governments.

In Myanmar, trends toward greater political freedoms have translated to a limited move toward freedoms online. A law requiring political news to be vetted by state authority prior to publication has been abolished, although restrictions on online content remains through the 2004 Electronic Transaction Law. The OpenNet Initiative (ONI) has noted a reduction in filtering in Myanmar after testing performed in August 2012.

The Trinidadian government requested that Google take down 10 videos from YouTube, which show Prime Minister Kamla Persad-Bissessar and Attorney General Anand Ramlogan in a variety of embarrassing situations. Google, who released its sixth Transparency Report in June, denied the request.

NETIZEN ARRESTS

A surge in the arrests of bloggers, activists, and ordinary citizens suggests that authorities are scrutinizing online content more than ever before. In Bahrain, the arrest and sentencing of prominent activist Nabeel Rajab for anti-government remarks on Twitter is one germane example of the threat faced by activists for their online activity. In Kuwait, a member of the royal family himself, Sheikh Meshaal al-Malek al-Sabah, was arrested for criticizing his family's policies on Twitter. Oman arrested several netizens for "defaming" the Sultan, a ruling made possible through Oman's Cyber Crime Law, which makes the publication of slanderous comments online an offense. Saudi Arabia's Anti-Cybercrime Law has been used to arrest web editors for providing venues in cyberspace for religious debate. In July, the United Arab Emirates conducted a series of sweeping arrests against bloggers accused of a variety of crimes, including the allegation of "colluding with foreign agents". Bloggers and netizens in Sudan and Algeria have also been detained this year. Tunisian blogger and critic of the ruling Ennahda party, Sofian Shurabi, was arrested — his is one of several arrests of bloggers in the country since the fall of the Ben Ali regime. While Shurabi was arrested under the charge of drinking alcohol in public during Ramadan and not directly for his writing, Amnesty International viewed the

arrest as part of Tunisian efforts toward curtailing "basic freedoms" and singling out anti-government activists for detention.

Iranian authorities are especially concerned with curbing the posting and accessing of inflammatory content on the Internet. According to Iran's Cyber and Information Exchange Police (FETA), Internet users can be arrested for promoting "lewdness," "evil doings" [Farsi], "Satanism" [Farsi], and blasphemous statements [Farsi] over social networking platforms, as well as for posting content offensive to Islam and Shiite Imams [Farsi] and content defaming government and Iranian officials [Farsi]. Satirization [Farsi] of Iranian religious and political topics and using VPNs [Farsi] are also illegal. Sattar Beheshti, a blogger who maintained the website My Life for My Iran and has criticized Iran's financial contributions to the Hezbollah movement in Lebanon, was reported dead [Farsi] a few days after being arrested by FETA. Although the details surrounding his death remain unclear, the dismissal of the commander of Tehran's branch of FETA [Farsi] indicates that the agency may be held responsible for his death. Iranian authorities, who are particularly sensitive to foreign criticism of its human rights record, announced that a parliamentary committee is currently conducting an inquiry.

In Egypt, a teacher was arrested for blasphemous comments posted on a Facebook page that he moderated. The teacher, however, claimed that the page had been hacked. Similarly, Indonesian authorities arrested Alexander Aan, a former civil servant who is now serving two years imprisonment for "blasphemy" after declaring his atheism on Facebook.

Authorities in Southeast Asia have also penalized bloggers for criticizing political leadership. Lèse majesté arrests have been common in Thailand where netizens have been arrested for allegedly anti-monarchist statements. A blogger in Malaysia was arrested this year for allegedly criticizing a local sultan. A report coming from Myanmar has claimed that an officer in the Myanmar Air Force was arrested and tortured for posting articles online critical of the country's military. Vietnam has similarly arrested songwriters for posting songs on the Internet deemed "anti-state propaganda" by authorities.

The trend of governments suppressing criticism from bloggers extends to Latin America and the Caribbean. The number of Cuban bloggers arrested and detained for being critical of the government has grown since the beginning of 2012. In September, Orlando Pardo Lazo, a blogger and editor of the magazine Voces, was arrested and detained illegally by Cuban police for nine hours on the same day that he was scheduled to appear on a panel at an independent debate forum. That same month, three other journalists were arrested from the Hablemos Press Agency, including Calixto Ramón Martínez Arias, who now faces up to three years in prison for criticizing the president. Yoani Sanchez, another prominent Cuban dissident blogger who has been recognized internationally for her work, was arrested twice this year. The first arrest occurred as she was travelling to attend the trial of a man charged with the murder of another dissident and the second happened during a protest in which Sanchez was detained with 19 others. In both instances, she was released soon after her arrest.

In Peru, the blogger and activist Jorge Chávez Ortiz was detained for several hours for filming police officers. Police have placed Ortiz under watch for blogging about attacks on journalists opposed to a mining project in

the city of Cajamarca. This past summer, police attacked several journalists for attempting to report on anti-mine and other protests happening in the country.

CONCLUSION

There is continued threat to freedom of expression as governments monitor and restrict online content. As could be seen in the examples discussed above, religious and cultural norms often play a significant part in determining what is being filtered. Online commentary that are critical of the political elite are also subject to both censorship and punitive legal action.

As more countries adopt online and mobile services, they face an increased risk of cyber attacks. Some of them have adopted laws that purport to combat cyber crimes and terrorism. However, these laws also serve as conduit to curb citizens' rights and freedom.

Some countries have eased restrictions in the past year. Libya and Tunisia — both of which experienced upheaval in 2011 — were praised for their high degree of Internet freedom relative to other countries in the region. Myanmar, in addition, has embarked on a top-down political reform and allowed its citizens to access dissenting political content for the first time in years.

In countries that continue to stifle free speech, social media has created a venue for individuals to air their grievances. Citizens in Latin America and the Caribbean, Southeast Asia, and the Middle East and North Africa have used social media as a tool for organizing popular protests, monitoring government abuses, and mobilizing political support in elections. The widespread use of these tools, however, has also led authorities to crack down on those who disseminate inflammatory content for fear of triggering a societal chain reaction. Looking ahead to 2013, we forecast that the contentious and often embattled use of social media will intensify as Internet access expands throughout the Asian and African continents.