IPS

ASIA 16.05.2019 | Janjira Sombatpoonsiri

Weaponizing cyber law

Previously, autocratic regimes relied on legal and bureaucratic tools to impede civic activism. Now, they also use cyber law

Having watched popular protests, from the colour revolutions in the former Soviet Union to the Arab Spring, challenge their counterparts' power, the world's autocrats have been adopting legal measures aimed at incapacitating civic groups, including pro-democracy movements and human-rights NGOs. Among the most sweeping measures are those enabling officials to monitor and punish activists' online activities.

Though overt crackdowns by security forces remain a serious concern, in recent years, autocratic regimes have increasingly been relying on legal and bureaucratic tools to impede opponents. For example, many countries – including Cambodia, China, Egypt, Ethiopia, Jordan, Russia, Tanzania, Thailand, Uzbekistan, and Venezuela – have tightened restrictions on organisation registration, foreign funding, and public assembly.

Autocratic governments have also made liberal use of existing laws prohibiting vaguely defined crimes like defamation and sedition, as well as anti-terrorism legislation. And, now, they are adding cyber laws to their arsenals of repression.

Of course, most countries have enacted laws addressing cybercrimes, privacy protection, and online financial transparency, and, for good reason. But autocratic regimes often craft such laws to keep their opponents in check – in particular by keeping the language ambiguous.

For example, in identifying who poses a cyber threat, such laws might refer to groups or individuals with 'malicious intent,' or those who seek to 'oppose the state,' 'endanger national security or ideology,' 'distort information which causes public panic,' 'advocate homosexuality or lesbianism,' or 'generate anti-state social movements.' Such broad definitions enable autocrats to portray virtually any dissident as a security threat, thereby providing an excuse – and even galvanising public support – for repression.

Look at Southeast Asia

Southeast Asia offers many examples of this trend. Various forms of autocracy prevail in seven of the Association of Southeast Asian Nations' ten member countries: competitive authoritarianism (Cambodia, Singapore, and Myanmar), single-party rule (Laos, Vietnam), absolute monarchy (Brunei), and military government (Thailand). Until 2018, Malaysia was in the competitive authoritarian category.

Over the last decade, these countries have augmented their dissent-stifling legislation with computer-related and cyber-security laws, all of which follow a similar script. Cambodia's cyber law, enforced by a new cybercrime unit, uses ambiguous language to facilitate the suppression of free speech. In Singapore, this function is served by the Internet Code of Practice and recently the Protection from Online Falsehood and Manipulation law. In Myanmar, it is achieved with the 2000 web regulations, which limit what can be posted online; the 2013 Telecommunications Law, which criminalises online defamation; and the 2004 electronic transactions law (amended in 2013), which imposes heavy penalties for a long list of nebulous offenses.

Similarly, laws purportedly aimed at preventing the spread of false information – such as Article 65 of Laos's criminal code – have been used against opponents. During the 2018 election campaign in Malaysia, the ruling party enacted an anti-fake-news law to emasculate the opposition, which won anyway.

For activists, pushing back against draconian cyber laws and other forms of digital repression will not be easy, not least because it remains uncharted territory.

A key component of these repressive cyber-strategies is expansive surveillance. Thailand's recently-enacted cyber-security bill – which complements the Computer Crime Act, adopted in 2007 and revised in 2016 – authorises the state to expand surveillance and strengthens its hand against vaguely defined cyberattacks. The Thai government – like those in Azerbaijan, Malaysia, Morocco, and Qatar – has reportedly purchased spyware from companies, including the Italy-based Hacking Team, that would allow them to hack into citizens' computers, mobile phones, and even GPS systems.

Data-localisation requirements – which compel tech firms to store their citizens' data on local servers – facilitate these efforts. Vietnam – along with China, Nigeria, Pakistan, and Russia – recently introduced such

requirements, supposedly to prevent data theft. But keeping data within a country also allows governments to exercise control over it.

Vietnam's cyber-security law, which took effect in January, allows the government to access locally-stored social media data and remove content deemed to oppose the state. China takes this a step further: with its vast resources, it is able to use advanced artificial intelligence to analyse the data that flow in, and thus to monitor its citizens.

In addition to legal repression, the use of fake videos ('deepfakes') and troll armies helps governments propagate their agenda and discredit activists. Cyber trolls in Thailand, the Philippines, and Vietnam reportedly engage in systematic bullying of online dissidents.

Activists try to push back

Activists across Southeast Asia and in autocracies worldwide are feeling the effects of these initiatives. Malaysia's Communications and Multimedia Act was used to prosecute individuals for criticising the authorities or monarchy in at least 38 cases in 2017. In Myanmar, more than a hundred cases have been litigated under the Telecommunications Law since 2013, and in 2016 alone, 54 people were prosecuted and eight imprisoned for dissension on social media.

The Thai junta has jailed several dozen citizens for sharing 'sensitive' information on social media sites. With the 2019 election approaching, it has used the Computer Crime Act to press unfounded charges against opposition parties, while turning a blind eye to its trolls' fake news. In Vietnam, where hundreds of dissidents were charged in 2017-18 for alleged anti-state activism both online and off, the new cyber-security law will only make matters worse.

For activists, pushing back against draconian cyber laws and other forms of digital repression will not be easy, not least because it remains uncharted territory. But that has not stopped some from trying. And, already, protests such as those in South Korea have had some success in inducing increased legal oversight. Many civic education groups have also been promoting digital literacy, so that citizens can help monitor the abuse of cyber laws.

At the international level, advocacy networks have lobbied democratic governments and international organizations to put pressure on autocratic regimes. But there is also a broader need for a coordinated global response aimed at protecting civic space. Only through sustained public pressure can we hope to persuade autocratic regimes to revise, or

reverse, their cyber policies.

(c) Project Syndicate



Janjira Sombatpoonsiri
Bangkok

Janjira Sombatpoonsiri is a research fellow at the German Institute of Global and Area Studies (GIGA) and an Assistant Professor at Thailand's Chulalongkorn University.