Thailand’s new Cyber Security Bill: security from military perspective

Submitted on Tue, 3 Apr 2018 - 01:29 PM

The coordinator of the Thai Netizen Network analyses the latest draft of the Cyber Security Bill, saying that the definition of “cyber” is too broad, there is a risk of offending over content affecting security, the Committee is structured to give dominant power to the security sector, and private agencies not complying with requests for data may be penalised, but state requests for data do not require any court order.

“Cyber security is the security of general infrastructure systems, whether it’s finance, the economy, society, daily activities or the military. But for this bill, when you look at the power structure of the committee in terms of checks and balance, it is like we’ve regressed to the time when the military was in power. They are using only the perspective of military security, mainly with regard to defending the nation. They’re not looking at other dimensions.”

This is one of the conclusions from the analysis by Arthit Suriyawongkul, coordinator of the
Thai Netizen Network, of the latest Cyber Security Bill.

Prachatai invites readers to analyse the broad definition of "cyber" that is broad enough to cover data and content, thereby risking offences concerning content that affects security; the committee structure that seems to give power to the security sector; a military fast track while civilians have to meet criteria to become officials; and requests for data which, if they not complied with, may result in legal penalties.

The broad definition of "cyber" entails the risk of offences over content affecting security

Arthit spoke of Article 3 on the definition of “cyber”. In this bill, the definition is “activities related to computer networks, computer systems, computer data communication and computer data.”

“Which is very broad. It could be anything. It includes the content read by people, not just the system. This is like the Computer Crime Act. We say that, in principle, the Computer Crime Act was designed for computer crimes like attacking the system, but Article 14 of the Computer Crime Act includes messages, images, and information read by humans, not just data read by computers. Therefore it also includes defamation and false data. Even though they excluded defamation in the last draft, false data remains. This kind of language reappears in the Cyber Security Act. Do the words “computer data” mean that if there are any video clips, images or messages widely disseminated on the Internet, this committee will say that it is a threat to cybersecurity? They then might order all ISPs
Thailand’s new Cyber Security Bill: security from military perspective ...

Arthit stated that this isn’t just his own interpretation. If we read a 2012 military commission report, there is a study by the Senate military commission which talks of a new form of threat that comes with social media and indicates what they are. A number concern attacks on the system and one relates to content that criticises or affects the fundamental institutions of the nation, which could be considered a cyber threat. It’s possible that this draft will be used alongside Article 14 of the Computer Crime Act.

The coordinator of the Thai Netizen Network explained that from now on if there are posts on Facebook criticising politics, institutions or criticising something like the 20-year national strategy or mocking the Prime Minister, causing misunderstandings, they might claim that discrediting the Prime Minister affects national security. For example, people uploading millions of video clips wouldn't cause the system to crash – it’s not a problem of the system. However, that video clip may upset people. It should be clearly stated that cybersecurity is the security of computer systems and information systems. As for the issue of upsetting people affecting national security, that should be dealt with in another law, not this one.

Arthit also explained that this Act can even be used in advance. For the Computer Crime Act, the incident must happen first, while the Cyber Security Act also covers prevention of any incidents. If there are suspicions that any person is going to disclose any data, they can be arrested on the premise of preventing the incident. The current draft can be interpreted as such, and it shouldn’t be like that. How should the Act be written so that the issue of content will be excluded, with only the issue of systems covered?

**Committee structure: leading power with the security sector**

Regarding the structure of the National Cybersecurity Committee, Arthit said:

When compared to the proposed draft two years ago, this section has changed quite a lot. In the former draft, the committee chair was the Minister of Digital Economy and Society, with no more than ten committee members. However in this draft, the Prime Minister is the chair, and the number of committee members is increased by including ministers from various ministries, security agencies, and other agencies. The position of deputy chairs was also added, with the Minister of Defence as first deputy chair, and the Minister of Digital Economy and Society as second deputy chair. So when the chair is unable to attend meetings, the first deputy chair will chair the meeting according to precedence. So the Minister of Defence will hold more power than the Minister of Digital Economy and Society. Moreover, if we look at the proportion of members who come from the security agencies, such as the National Intelligence Agency and the National Security Council, this
has increased.

Arthit further explained the committee according to this draft, there will be two committees, the "National Cybersecurity Committee", taking care of policy-making, and the "Executive Committee", implementing the policies. In this aspect, if we look at this overall, the security side and the defence side will be the ones looking at policies while the role of the Ministry of Digital Economy and Society, which previously was making the policies, now becomes an implementation of the policies.

2 models regulating cyber plans; the security side takes care of policy, and the Ministry of Digital Economy and Society leads in implementation

For the model plan that will be regulating relevant policies, the coordinator of the Thai Netizen Network explained that no matter what policy is made by the National Cyber Security Committee, according to Article 5 of the bill, all policies must be in accordance with the 2 model plans. The first model plan concerns the development of the digital economy and society of the National Digital Economy and Society Committee with the Prime Minister as chair, and the second concerns the security of the National Security Council.

This means underneath there will be the cybersecurity plan and above there will be two more model plans which regulate the cybersecurity plan. In the power balance, even though the National Cyber Security Committee can return suggestions to the National Digital Economy and Society Committee, it cannot send suggestions to the National Security Council. Also taking in mind the proportion of security officials that are on the National Cyber Security Committee, it all becomes clear that in this draft the power is not with the Ministry of Digital Economy and Society, but with the National Security Council and the Ministry of Defence," said Arthit.

Arthit gave an example of the situation from other countries. When we look at the security councils or the ministries of defence in foreign countries, they are led by civilians. But in our country for some reason, the National Security Council is led by the military, while past Defence Ministers in Thailand have mostly held military positions, not completely separated from the army.

If the private sector does not comply with requests for data, it may be penalised – requests for data do not require court orders
The coordinator of the Thai Netizen Network talked about further problems of this bill. The mechanism used to check the exercise of powers is rather unclear. In the case of asking for cooperation with requests for data, the court may be asked to issue an order, but only for cases where the private agency does not consent to the request. Therefore if the private agency consents, a court order is not needed, while state agencies can be directly requested without a court order. We see there should be no exceptions here. No matter what kind of data is involved, whether from a private or state agency, or whether they consent or not, the court should always be consulted, since, in the end, the data may not be theirs. For example, suppose they want data from a certain bank. That data belongs to the bank or the bank’s customers, and if the bank consents, a court order is not needed. Thus, the bank may consent to give the data.

Article 7 Clause 2 states “In the case that the private sector does not comply with the order of an official requesting cooperation let it be proposed to the committee to consider proposing to the overseeing state agency to consider punishment according to any law, announcement or other regulation in existence.”

Arthit explained that under this Article if any agency does not cooperate, they may receive punishment. That’s why, for the issue of consent or no consent, when in the end there is a punishment in place, it is no longer voluntary. In this situation, the balancing power mechanism, here the court, will not be used, since the private sector would consent rather than risk punishment. In this case, there should be a clear distinction. For any cases concerning requests for cooperation, there should be no punishment, but in serious cases, orders must be issued, and non-compliance with an order will be punished as a refusal to obey an order.

**Definition not concise, state agencies may not be just state agencies**

Concerning the fact that requesting data from state agencies doesn’t require a court order, Arthit said that, when we take a look at the definition in Article 3 of “state agency”, it refers to the central government, regional government, local government, independent agencies, public organisations, state enterprises and state agencies established according to Acts or Royal Decrees. It also includes legal persons, groups of persons, or persons who hold power in state operations in all cases. This could include private agencies that have been granted concessions from the state, so the BTS could also be covered. This is because it is not clear as to what agencies are included. It may be too much to clearly name the agencies, but there was a proposal that suggested a clear announcement of agency names that are really important. It doesn’t need to be in this bill but indicates in the bill that agency names can be referred to according to the announcement since at least we know beforehand which agencies will be important.
The military gets the fast-track, civilians must meet criteria to become officials

Article 49 on the appointment of officers according to this Act, has the minister appoint experts in computer systems or information security protection with the qualifications as specified by the minister.

Article 50 for the benefit of coordination or implementation, has military officials of the Ministry of Defence that has been assigned to missions responding to and dealing with cyber threats that will affect security, as responsible officials according to this Act.

Concerning Articles 49 and 50, Arthit stated that the appointment of officials could be divided into two. One is the normal method where the Prime Minister appoints experts according to the specified criterion. Second is what we call “fast-track”. It is a special method, an urgent method. Any assigned military personnel can become officials according to this Act instantly and automatically, without needing to meet the criterion of being an expert. Therefore it can be seen that even in practice the standards applied to the military and civilians are not equal.
Thailand’s new Cyber Security Bill: security from military perspective ...

Cartoon by Stephff: Prayut's submarine in Isaan

The tale of Abdullah Isomuso – Not a movie

Greta Thunberg and Fridays for Future receive Amnesty International’s top honour

Tweets by prachatai_en
Economics Links
- Bretton Woods Project
- Focus on the Global South

Media Links
- The Southeast Asian Press Alliance (SEAPA)
- UPI Asia Online
- FACThai
- Asia Sentinel
- Inter Press Service News Agency
- Global Voices
- IFEX
- Counter Punch
- Engage Media
- International Federation of Journalists
- Global Investigative Journalism Network

Academic Links
- The New Mandala
- The International Institute For Strategic Studies
- Kyoto Review of Southeast Asia

Support Prachatai

About Prachatai.com | Code of Conduct | independent web newspaper

© The Foundation for Community Educational Media 2006 (cc) BY-NC