ASIA CENTRE
centreasia.eu

DGRIS

Compte-rendu

OBSERVATOIRE ASIE DU SUD-EST 2017/2018

Cybersecurity in Southeast Asia

Compte-rendu de la table ronde du 22 mai 2018
par Benjamin Ang, RSIS (Singapour)
Table-ronde 5/8, Observatoire de l'Asie du Sud-Est, cycle 2018-2019

Participants :

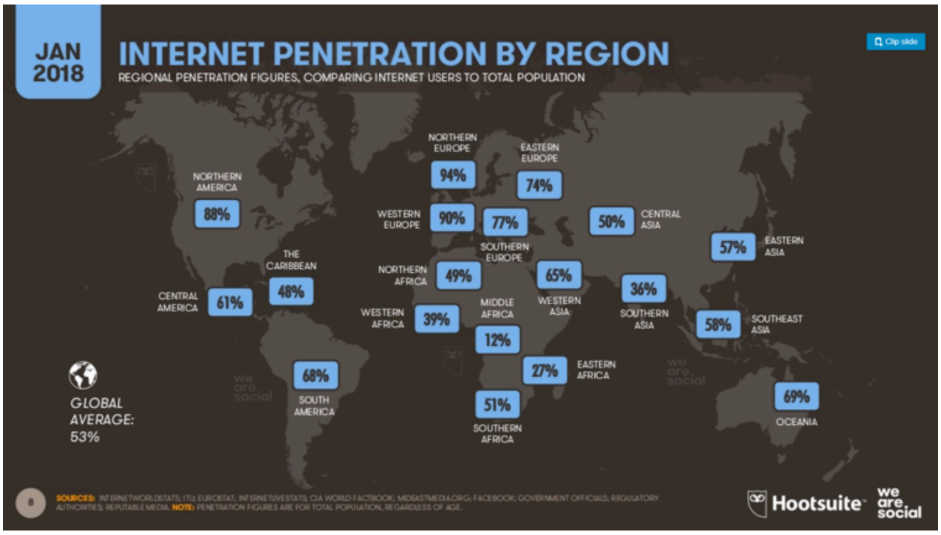
- Speaker : **Benjamin Ang**, Senior Fellow, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore
- Chair : **Jean-François di Meglio**, President, Asia Centre

Maison de la Recherche de l'Inalco
2 rue de Lille
75007 Paris - France
Tél. : +33 1 75 43 63 20
Fax. : +33 1 75 43 63 23
www.centreasia.eu
contact@centreasia.eu
siret 484236641.00037

Introduction : Digital Economy of Southeast Asia

The digital economy of Southeast Asia is growing rapidly. According to **Benjamin Ang**, this brings about tremendous opportunities to countries in the region but also comes with many risks and challenges. To set the picture, 58% of its population has now access to internet, which sets it quite above the global average, and the region also boasts a disproportionate mobile connectivity of 141% – that's more mobile phones than humans. This increase in internet use makes the region more prone to cyber-attacks and other cybersecurity threats. This huge growth of the digital economy should actually be accompanied with the same kind of growth in cybersecurity awareness. For Benjamin Ang, ASEAN countries are "in it" for the benefits, such as goods and services, but forget to put security on the forefront. For instance, with the development of e-commerce and mobile transactions in general, such as in the Philippines, the "rush to mobiles" needs to be paired with the improvement of traditional internet web access. Indeed, without the development of cyber norms of behaviour, the region's lack of governance, skilled capacity and attribution capability could potentially act as catalysts for cyber incidents and cyber-enabled information conflicts in the region. Singapore, Malaysia, the Philippines and Indonesia are particularly at risk with Singapore all the more vulnerable due to its over-reliance on technology.

Furthermore, Benjamin Ang reminds us that ASEAN countries have also been used to launch attacks, either due to the exploitation of their unsecured infrastructure, or the use of their well-connected hubs for initiating attacks. In fact, every country in ASEAN has had a major cyber-attack. Even high-tech Singapore, for example, has had massive website defacement, including that of the PM's which was not done by any elaborate activist organisation, but simply by an individual making use of the city-state's digital weaknesses. This led to the formation of a cybersecurity agency and a cybercrime unit in the police force. Vietnam Air was also hacked by a Chinese hacking group and Indonesia experiences more than 50,000 cyber-attacks daily (more examples in the introductory note to the roundtable). Because of this increased exposure to cybersecurity threats, ASEAN member states support the development of cyber norms, with Singapore heading the fight by committing substantial resources to its own national Cybersecurity Strategy. However, with cyber risks impeding trust between member states and preventing countries from realising their full digital potentials, challenges remain.

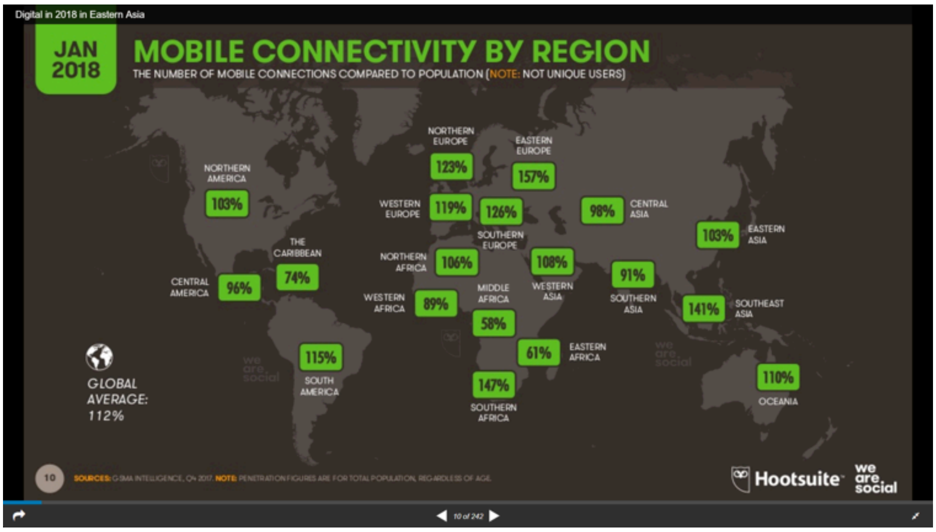


JAN 2018

INTERNET PENETRATION BY REGION

REGIONAL PENETRATION FIGURES, COMPARING INTERNET USERS TO TOTAL POPULATION

SOURCES: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION, REGARDLESS OF AGE.



Digital in 2018 in Eastern Asia

JAN 2018

MOBILE CONNECTIVITY BY REGION

THE NUMBER OF MOBILE CONNECTIONS COMPARED TO POPULATION (NOTE: NOT UNIQUE USERS)

SOURCES: GSMA INTELLIGENCE, Q4 2017. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION, REGARDLESS OF AGE.

Challenges for Cybersecurity in Southeast Asia

Mainly, there is a lack of a standardised strategic mindset and a unifying framework regarding cybersecurity. Indeed, only a third of ASEAN member states have a clearly defined strategy, and they are mostly treated as military issues, which unfortunately treats only half of the problem. It is in fact often unclear who's in charge. Responsibility may often be split between national police, for cybercrimes, interior ministry, for critical infrastructures, telecommunications ministry, for breaches, and the military, for cyber conflicts, with little, if any, coordination or continuity. This often results in underinvestment. Policy preparedness and institutional oversight are in fact crucial when it comes to cybersecurity. Linked to that is the fact that Cyber risk is still perceived as an IT problem, and not as a strategic or a business one. Thus, no substantial budget is allocated to the issue and regional businesses do not have a comprehensive approach to cybersecurity. Furthermore, the region's cybersecurity industries tend to struggle to meet demand due to their lack in capability and expertise, while growing interconnectedness between the region's economies and the ever-evolving technologies will only intensify this systematic risk. Like hacking into a casino through the aquarium's thermometer, Benjamin Ang argues that interconnected digital economies are only as good as their weakest access point. Last but not least, the lack of trust between countries, already exacerbated by the pervasive suspicion triggered by cyber threats, tends to impede the sharing of threat intelligence amongst neighbours which would be a first step towards tackling this region-wide critical issue.

Cyber-enabled Information Conflicts in East Asia

According to Benjamin Ang, if cyber-attacks and hackings are worrying, what causes even greater concern are cyber-enabled information conflicts. With regional conflicts in the Asia-Pacific region already transcending into the cyber and information domains, information operations with lower risks of escalation can indeed now replace military commitments in the region's security flashpoints: namely, the struggle for dominance between China and Japan, the future of the Korean Peninsula, intra-regional competition in territorial disputes in the East and South China Seas, and the long-term regional strategic competition between China and the United States. The key idea behind this is that online operations can have offline impacts.

- First, cyber-enabled information operations can be used to deny or create political outcomes without any visible military involvement, even if sceptics argue that there are serious limitations with regard to the use of cyberspace for political purposes.
- Second, the growing interdependencies brought by technology in all aspects of governance has rendered traditional conceptions of deterrence and defence vulnerable to strategic surprises, with the emergence of asymmetric forms of information and cyber warfare.
- Third, cyber-enabled information operations can serve as a key enabler and force multiplier of physical operations, enabling actions, capabilities and effects of land, sea, air, and space operations.
- Fourth, information operations create cognitive effects shaping perceptions and online behaviours with offline consequences, thereby influencing, for example, what people buy or how people vote. Through a new cyber-enabled domino effect, propaganda is already in the hands of the citizens and can be disguised as a message from a friend.
- Fifth, online capabilities evolve parallel with military-technological advances, such as electronic miniaturisation, additive manufacturing, nanotechnologies, artificial intelligence, space capabilities, and unmanned systems that alter the character of future warfare.

For China, achieving air and naval superiority in the region is dependent on the Chinese People's Liberation Army's ability of achieving "information dominance" (*zhi xinxi quan*), by controlling the electromagnetic spectrum, while prioritising computer network defence. In this context, while Beijing has been wielding economic leverage and "soft power" diplomacy as primary means of power projection, the PLA has also been actively exploiting strategic information operations to direct influence on the process and outcome in areas of strategic competition, guided by its conceptual umbrella for information operations: the "Three Warfares" (*san zhong zhanfa*). This concept is based on three-mutually reinforcing strategies:

- the coordinated use of strategic psychological operations,
- over and covert media manipulations,
- and legal warfare designed to manipulate strategies, defence policies and perceptions of target audiences abroad.

The strategic competition for research and development of cutting-age military technologies and cyber capabilities that enables the PLA to fight its information conflicts and achieve information dominance is embedded in the concepts of military-civil integration (*junmin ronghe*) and civil-military integration (*yujun yumin*), which promotes the development of dual-use technologies and combined defence and civilian industrial bases. This has been elevated into a national-level strategy by President Xi Jingping: "the integration of civilian and defence development will involve multiple fields and enable economic progress to provide greater material foundation for defence construction".

In fact, Benjamin Ang argues that, embodied by the country's 50 Cent Party and its Internet Water Army, there is a much greater cooperation and interactions between civil and military actors in China than in the western world, which can blur the line between peacetime and wartime. Indeed, China's strategy also relies on foreign acquisition of targeted dual-use technologies, resources and knowledge, such as engines, microprocessors, control systems, enabling technologies, advanced diagnostic equipment and computer-assisted design, which consistently raises tensions in the Sino-US relations. According to James R. Clapper, the Director of National Intelligence, addressing the Senate Armed Forces Committee, “China continues to have success in cyber espionage against the US government, our allies, and US companies”. In East Asia, strategic competitions are defined by how capable regional powers are at wielding non-military methods such as political, economic, information and military pressure during peacetime. In a way, the confluence of advanced cyber and information warfare strategies creates new weapons of mass effectiveness. For instance, the weaponisation of social media provides tools for both state and non-state actors to seed ideas, tailor information, influence perception and thus, shape strategic outcomes of conflicts before they actually happen. The end game of such information operations is to manipulate the adversary’s perceptions, shape its division-making process and strategic choices, while minimising the scale of kinetic force, in peacetime like in wartime.

Cyber Norms and ASEAN

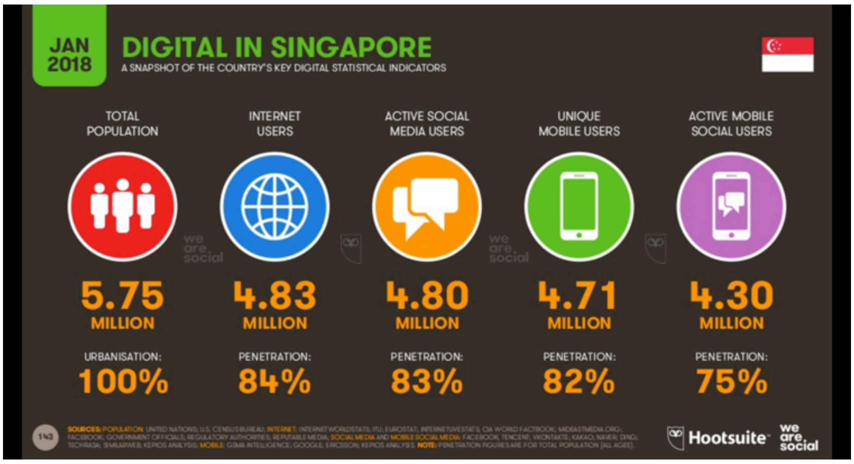
Cyber-attacks and cyber-enabled conflicts run the risk of escalating into larger conflicts, especially in Southeast Asia, where countries lack the means of accurately attributing the true source of cyber operations. At the moment, “anything goes” in cyber space, and with attacks routed through any number of hubs in third party countries and the difficulty of tracking cyber-attacks back more than one hub, the risk of wrong attribution is indeed high and spreads mistrusts amongst neighbours. As a result, ASEAN member states have been looking at the development of cyber norms of behaviours and confidence building measures to create a rule-based cyberspace.

As a matter of fact, Benjamin Ang reminds us that norms reflect the international community’s expectations, set standards for responsible State behaviour, allow the international community to assess the activities and intentions of States, and have a long-standing history of reducing conflict between states. Internationally, the development of cyber norms has been led by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), comprised of 25 countries. After affirming in 2013 that international, and particularly the UN charter, applies to cybersecurity and is “essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment”, the UNGGE agreed on 11 good practices and limiting norms two years later. However, the realistic application of certain norms, such as the ban of proxies, remains unclear and idealist. With the lack of clarity and consensus on the implementation of the agreement amongst members, Benjamin Ang argues that a global consensus on cybersecurity norms is unlikely to materialise in the near future. Problems areas arise when addressing issues such as the right to respond to internationally wrongful acts, the right to self-defence, and international humanitarian law. As a result, the development of international cyber norms has indeed stalled for now. As a result, regions like ASEAN are trying to develop regional agreements instead. At the ASEAN ministerial conference on cybersecurity in 2016, ASEAN member states have indeed agreed on the value of developing a set of practical cybersecurity norms of behaviour in the region, while supporting the development of basic, operational and voluntary norms, set out in the UNGGE 2015 report. Taking into account the fact that the majority of critical infrastructure is held by private companies and uses private sector software, hardware and services, Benjamin Ang recognises the need for a multi-stakeholder approach, with academia, business and civil society working together to create a more wholesome and holistic approach to cybersecurity norms.

Case Study: Singapore’s Cyber Threat Landscape and Cybersecurity Strategy

Due to its high level of internet connectivity, Singapore is particularly susceptible to cyber-attacks, listing SMEs, individuals and Critical Information Enterprises, including the Government, Healthcare, Banking and Finance sectors, amongst its victims. Benjamin Ang tells us that, in 2016, prevalent cyber threats observed in the city-state were:

- Ransomware, with thousands of computers and mobile phones hit by WannaCry and Petya;
- Website Defacement, with 1,750 reported cases in 2016 alone;
- Phishing, with 2,512 phishing URLs with a Singapore link found;
- and Command and Control servers, 60 of which were observed within Singapore’s cyberspace, capable of conducting malicious activities such as data theft, spam campaigns and denial of service attacks.



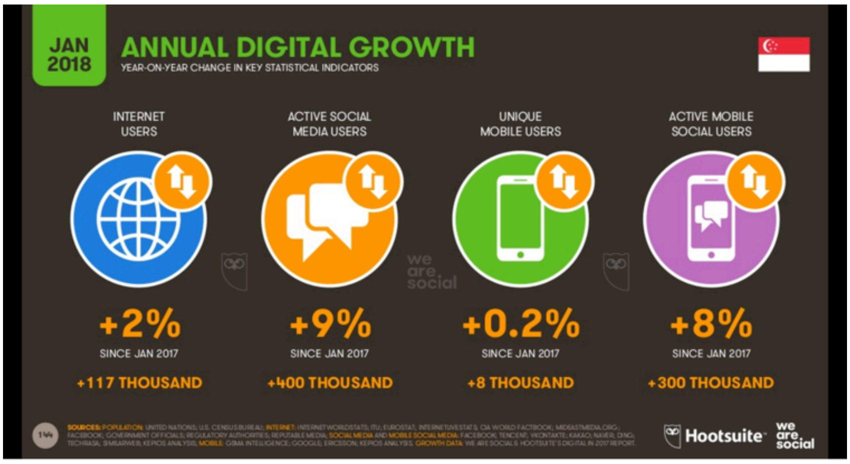
JAN 2018

DIGITAL IN SINGAPORE

A SNAPSHOT OF THE COUNTRY'S KEY DIGITAL STATISTICAL INDICATORS

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
5.75 MILLION	4.83 MILLION	4.80 MILLION	4.71 MILLION	4.30 MILLION
URBANISATION: 100%	PENETRATION: 84%	PENETRATION: 83%	PENETRATION: 82%	PENETRATION: 75%

143 SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).



JAN 2018

ANNUAL DIGITAL GROWTH

YEAR-ON-YEAR CHANGE IN KEY STATISTICAL INDICATORS

INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
+2%	+9%	+0.2%	+8%
SINCE JAN 2017	SINCE JAN 2017	SINCE JAN 2017	SINCE JAN 2017
+117 THOUSAND	+400 THOUSAND	+8 THOUSAND	+300 THOUSAND

144 SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. GROWTH DATA: WE ARE SOCIAL & HOOTSUITE'S DIGITAL IN 2017 REPORT.

Singapore based its Cyber Security Strategy in 2016 around four pillars:

- building a resilient infrastructure;
- creating a safer cyberspace through the mobilisation of businesses and the community;
- developing a vibrant cybersecurity ecosystem comprised of a skilled workforce, technologically-advanced companies and strong research collaborations;
- and strengthening international partnerships.

As a result:

- Singapore pledged to help forge international and ASEAN cooperation to counter cyber threat and cybercrime through the ASEAN Regional Forum, the ASEAN Network Security Action Council (ANSAC), the ASEAN CERT Incident Drill (ACID), and the Interpol GCI (Global Complex for Innovation), hosted by Singapore.

- The City-State also endeavours to champion international and ASEAN Cyber Capacity building initiatives with the launch of a S$10m ASEAN Cyber Capacity fund to help fund efforts to deepen cyber capacities across ASEAN member states.

- Third, Singapore's strategy vows to facilitate exchanges on cyber norms and legislation by hosting events such as the ASEAN Ministerial Conference on Cybersecurity, the international Cyber Leader' Symposium and the ASEAN Cybercrime Prosecutors Roundtable Meeting during Singapore's International Cyber Week events.

- Finally, Singapore also runs programmes with partner countries, such as the ASEAN Cyber Capacity Development Project, the Singapore-United States Third Country Training Programme, and the ASEAN+3 Cybercrime Workshop, with China, Japan and South Korea.

Building a Resilient Infrastructure

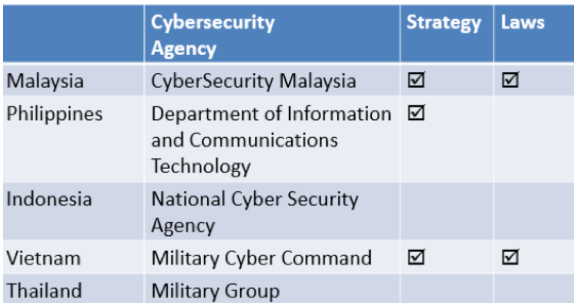
Creating a Safer Cyberspace

Developing a Vibrant Cybersecurity Ecosystem

Strengthening International Partnerships

Other Southeast Asian Responses

If Singapore has made a lot of progress regarding cybersecurity norms and strategy, Benjamin Ang reminds us that the other Southeast Asian nations have varying degrees of cybersecurity maturity. In fact, in addition to Singapore, only Malaysia, the Philippines and Indonesia have clearly defined government agencies dedicated to their country's cybersecurity – it is still an issue left to the Defence and the Military in Thailand and Vietnam, which focuses merely on a military approach. Only the Philippines, Malaysia and Vietnam have a clearly defined cybersecurity strategy, according to Benjamin Ang, while only the latter two have proper legislation. Indeed, after Singapore, Malaysia has been hailed as one of the most progressive ASEAN nation in terms of cybersecurity strategy.



	Cybersecurity Agency	Strategy	Laws
Malaysia	CyberSecurity Malaysia	☑	☑
Philippines	Department of Information and Communications Technology	☑	
Indonesia	National Cyber Security Agency		
Vietnam	Military Cyber Command	☑	☑
Thailand	Military Group		

Concluding Remarks

In conclusion, faced with the limited progressed made across the rest of the region, Benjamin Ang recommends that ASEAN member states need to clearly establish government agencies that are officially responsible for the development of cybersecurity policy to drive the development of cyber norms from within their states, and develop capacity in Track 2, to discuss further cooperation and the development of cyber norms, in order to support the efforts at governmental level.

As ASEAN chairman in 2018, Singapore announced that it endeavours to connect ASEAN people and economies in a network of smart cities as well as to enhance the region's cyber security strategy.

Questions and Discussion

Concluding this exhaustive and comprehensive presentation, **Dr Éric Frécon** opened the floor to the many participants. Regarding the risk increased cyber security could have on the region's democracies and their civil liberties, **Benjamin Ang** acknowledged the fact that considering the laws designed to protect key infrastructures, in some instances, radicalisation and security issues have been lumped together with anti-government messages, and even pornography, which could have worrying political and social impacts on the long run.

Questioned about the intensification of the cyber threat coming from China, our speaker replied that, for example, the South China Sea was one incident that flared up because in this instance, China and Singapore came head to head, with the Singapore PM having to face serious backlash online. Cyberwar is indeed a war, even without guns, that started a long time ago; the technologies have simply evolved. If certain countries, like Australia, have declared they were an offensive cyber power, Benjamin Ang argues that it is better to remain strategically ambiguous. For instance, France believes it is better to be prepared to react than to be offensive, as we have seen with the cyber attacks hours before the strikes on Syria. Affirmed by a representative of the French Ministry of Armed Forces, France doesn't disclose its own attacks and counter measures, unlike the UK for example. It is a political question.

Finally, with regards to the limited progress on the development of international cyber norms and legislation, our distinguished panel drew similarities between the sea and cyberspace – with the law of the sea taking more than 30 years to take shape. Cyberlaw needs time as well.

Roundtable report by Tom Eisenchteter, Asia Centre