# Asia Cyber Diplomacy Workshop

## Diplomacy: Between Tradition and Innovation

### Workshop Report


Cyber diplomacy is vital for avoiding miscommunication and conflict in global Internet policy and maximising potentials for cyber agreements. This was the echoing point of the Asia Cyber Diplomacy Workshop, attended by 30 diplomats and other officials from 14 countries.

The workshop's participants gained knowledge of digital policy and acquired skills through a blend of showcases of the Internet's present and future, presentations and engaging discussions by global and regional experts, and a simulation exercise on negotiating an International Declaration concerning the Internet facilitated by senior diplomats.

The training was adjusted to the regional specificities of Asia and, in particular, ASEAN countries. Participating diplomats were immersed in interaction with participants from civil society, academia, and the business sector. Regional cross-fertilisation was enriched by the participation of diplomats from several non-Asian countries, including Mexico, Ireland, and Peru.

## Key points and proposed actions

This section summarises the key points that recurred throughout the workshop and the informal discussions. The list of proposed actions is based on Diplo's experience in training activities in other regions.

| Key points | Action |
|---|---|
| In ASEAN countries, the main focus is on the digital economy. Legal, security, human rights, and the cultural aspects of cyber diplomacy are less covered in policy-making. | Promote a holistic approach to cyber diplomacy (economic, technical, legal, security, etc.) through awareness-building and training activities. |
| There is a lack of national coordination on cyber diplomacy issues. | ♦ Promote a whole-of-government/country approach to digital policy.<br>♦ Involve officials from other government departments dealing with foreign aspects of cyber issues (security, economy, culture) in training activities.<br>♦ Promote national Internet Governance Forums as a way to bring different policy communities together. |
| Same issues – different terminology. The interchangeable use of terms creates policy confusion related to who bears the responsibility of covering various aspects of cyber diplomacy at both national and international levels. | ♦ Create a comparative dictionary of cyber diplomacy and policy, with translations and semantic coverage of the main concepts in different languages (e.g. the meaning of Internet governance in English, French, Thai, and Chinese).<br>♦ Translate cyber policy, Internet governance, and diplomacy publications in the main languages. |
| There is a lack of organisational structure and human resources among ministries of foreign affairs (a lack of cyber sections or cyber ambassadors). | ♦ Share the practices of countries that have developed cyber diplomacy capacity (e.g. organise a global conference on cyber diplomacy).<br>♦ Provide training based on a blended-learning model (online and in-situ training; showcases, lectures, discussions, and simulations, etc.). |
| There is a lack of efficient training on cyber diplomacy and Internet governance. | ♦ Train trainers in order to ensure sustainability.<br>♦ Introduce cyber issues in the post-graduate curricula at universities in the region, including through cooperation with European training organisations and educational institutions.<br>♦ Organise a meeting with directors of Asian diplomatic academies at the next International Forum on Diplomatic Training (23-25 September 2015) in order to discuss the introduction of cyber diplomacy training in their respective academies. |
| There is a need for more coordination and knowledge exchange across the region. | ♦ Continue delivering two-day, intensive, blended-learning training sessions in the region.<br>♦ Introduce an interactive online learning and community facilitation platform for ASEAN countries, to enable continuous efficient and low-cost knowledge exchange. |

## Narrative report

The cyber diplomacy workshop started in the morning of 28 August in Pullman Bangkok Hotel G in Bangkok. While the workshop participants were entering the lobby and were welcomed with tea and coffee, Mr Vladimir Radunović, Director of Cybersecurity at DiploFoundation, provided the first CyberLab showcase – practical demonstrations of the Internet's increasingly futuristic elements, including the Internet of Things, Bitcoin, and 3D-Printing.

Having had this appetiser, the 30 participants moved into the workshop room, where Dr Jovan Kurbalija, Director of DiploFoundation, officially opened the event, accompanied by Ambassador Dhiravat Bhumichitr, Director of the Devawongse Varopakarn Institute of Foreign Affairs, and Mr Bernhard Kelkes, Deputy Head of the Embassy of the Kingdom of the Netherlands in Bangkok.

Ambassador Bhumichitr outlined the main challenges of the Internet for diplomats, and the need for diplomats to become 'masters of the Internet'. Subsequently, Mr Kelkes explained the increasing relevance of the Internet for diplomats, and the corresponding risk of digital security dilemmas that could give rise to a 'cyber arms race'. He also elucidated the Dutch interest in cybersecurity, which is no longer considered in purely technical terms, having entered the political, economic, and moral domains. Finally, he encouraged diplomatic cooperation as a very important way of promoting cybersecurity and stability.

After the welcome remarks, participants had a chance to get to know one another. They were asked to present the demographics of their group. It quickly became clear that there was a diverse participation in the room, from seasoned diplomats to more junior ones, academia, and civil society members.

Subsequently, Mr Radunović gave a basic introduction to the functionality of the Internet by looking under its bonnet, so to say. Participants gathered an initial understanding of Internet technology in order to address cyber diplomacy issues. In particular, his presentation focused on the physical infrastructure, critical Internet resources, and the Internet's cloud and content. It also clarified concepts related to protocols, such as IP numbers, domain names, and the role of ICANN.

Dr Kurbalija explained three triangles that are related to the Internet, covering the Internet business model, the politics around data, and the triangle balancing human rights, cybersecurity, and business interests.

Once this basic understanding of the Internet was established, Dr Alex Sceberras Trigona, Special Envoy of the Prime Minister of Malta and Former Minister of Foreign Affairs of Malta, explained the relationship between the Internet and diplomacy, as well as the ways in which the Internet could be categorised. He explained that it could be conceptualised as a 'matter of common concern', as a 'global public good', or even as the 'common heritage of mankind' – three different legal concepts with varying diplomatic consequences for the classification, categorisation, and regulation of the Internet.

After the coffee break, the workshop reconvened with a presentation about the applicability of international law to cyber challenges, given by Ambassador Kriangsak Kittichaisaree, member of the International Law Commission of the United Nations, who spoke using a video call from

Jakarta. Ambassador Kittichaisaree talked about many of the dilemmas posed by the Internet for International law, creating grey areas in different legal areas, including the concept of attribution (how to know whether a cyber attack can be attributed to a state) and distinction (how to distinguish between military and civilian Internet structures).

He further clarified that there was only one regional convention on cyber crime, the Budapest Convention, which increased legal dilemmas, since no international regime can be referred to when resolving legal issues about the Internet. After Ambassador Kittichaisaree's presentation, an animated discussion focused on the use of force and the right to defence in the context of cyber attacks, non-state actors, and suggestions to increase the participation of ASEAN countries in global Internet policy discussions. He referred to the second edition of the Tallinn Manual which will be discussed in February 2016 at the meeting in The Hague.

The after-lunch session addressed the question of WHERE cyber diplomacy is performed. Moderator Bart Hogeveen, fellow at the Clingendael Institute, introduced the topic and Dr Kurbalija provided a short introduction to the spaces of cyber discussions, including the United Nations General Assembly, the UN's specialised agencies, NGOs, and private standardisation bodies. Subsequently, Ms Jessica Woodall, analyst at the International Cyber Policy Centre, introduced research that has been conducted by her organisation, which examines the level of cyber maturity in the Asia-Pacific region, measuring cyber-related structures, policies, legislation, and the level of cyber social awareness of different countries in the region.

Mr Sameer Sharma, senior advisor of the ITU's regional office for Asia-Pacific, then outlined the ITU's Internet-related work in the Asia-Pacific region. Mr Hogeveen concluded the session and observed that there were three main topics that had been addressed: cyber governance, cybersecurity, and cyber development. He asked the panellists which international regime would states engage with if they faced specific problems of cyber attacks. Ms Woodall spoke about the utility of the ASEAN regional forum, while Mr Sharma summarised the broad range of initiatives that could be involved in cybersecurity, including CERTs, the ITU, UNODC, but also Child Help Lines and UNICEF, in cases related to child protection online. Mr Hogeveen then concluded that even though there is a good degree of cooperation and coordination at the technical level, we still need try to find one another at the policy and strategic level.

Another CyberLab took place during the coffee break. This time, Mr Radunović showcased and explained various types of cyber attacks such as the distributed denial of service (DDoS), and explained how botnets work. In an easy, relaxed, yet intellectually warmed-up atmosphere, participants came up with number of questions, and clarifications followed.

The following sessions addressed the question of HOW cyber diplomacy is performed using two case studies: ICANN and the Internet Governance Forum (IGF). Mr Wanawit Ahkuputra, Deputy Executive Director of the Electronic Transactions Development Agency, presented the policy complexity of the work of the Government Advisory Council (GAC) at ICANN. Countries have to find better ways of coordinating their cyber diplomacy approaches in dealing with ICANN's issues of public interest (protection of names, stability). In many countries, this link between GAC representatives and diplomats dealing with cyber issues is still weak or missing.

Mr Moedjiono Sardjoeni Matdullah, Senior Advisor at the Ministry of Communication and Information Technology of Indonesia, explained the main roles and objectives of the Internet Governance Forum, and presented the Indonesian experience in dealing with cyber diplomacy. For Indonesia, the main learning process was organizing a national IGF and hosting the global IGF. In this process, government, the business sector, and civil society learned in practice how to coordinate activities and work together. The subsequent discussion focused on the multistakeholder approach and its relationship to cyber sovereignty.

The first day concluded with the start of a negotiation simulation exercise, for which the participants were asked to form three groups and negotiate a cyber agreement. Ambassador Kishan Rana, a former Indian diplomat, introduced the simulation by providing theoretical and practical advice for successful negotiation, based on his own experience and the long history of international diplomacy. He also provided recommendations on effective chairmanship. By the end of the day, the three groups were well on their way to exploring the agreements, and the workshop dinner that took place that evening was a good place for continued informal negotiations.

On the second day of the workshop, the simulation exercise reconvened. After about 90 minutes, all three groups had managed to reach a compromise agreement. The groups' three mentors – Dr Kurbalija, Ambassador Rana, and Ambassador Sceberras Trigona – summarised the main developments of their groups and explained the process of reaching an agreement. Dr Kurbalija provided a reality check by comparing what was achieved in the simulation exercise to the real-life position of key players.


He explained that for all parties, a negotiated cyber agreement is preferable to most other alternatives. Without cyber agreements, countries risk disintegration of the Internet with serious economic and societal consequences. Thus, he was optimistic about reaching a future compromise. Well-developed cyber diplomacy would ensure that a deal was reached and not derailed by a lack of understanding and miscommunication.

After the negotiation exercise, Mr Aaron Boyd, Chief Strategy Officer at ABI Research, provided further information about benchmarking countries in the Asia-Pacific region, based on the Global Cybersecurity Index that has been developed by ABI Research and the ITU. He explained how this index came into being, and how the ranking can stimulate cybersecurity commitment on the part of individual countries. He provided several examples of countries in the region and their scores in the different areas of cybersecurity commitment. The subsequent discussion focused on measuring commitment and comparing states that differ in size and the attitudes of individual states towards the index.

The concluding session provided an overview of the different governmental departments that are connected to the global cyber diplomacy process. Dr Kurbalija was the session's main speaker, and he received additional input from Ambassador Sceberras Trigona and Mr Boyd. Together, they discussed the challenge of the coordination between the telecommunication, economic, defence, and foreign ministries in dealing with cyber issues. The importance of international cooperation and capacity building was once again emphasised, with an example of the Global Forum on Cyber Expertise established at the GCCS in The Hague earlier this year. Dr Kurbalija ended on an optimistic note, expecting that with sufficient empathy, listening, and substantive discussion, cyber diplomacy could ensure the containment of risks and could realise the potential of the Internet for economic and societal developments. With this in mind, the participants used the afternoon for bilateral consultations on developing cyber diplomacy capacities.

## Training methodology

The workshop was based on the interplay of three training methodologies:

- In the CyberLab, participants got direct experience of the main cyber issues such as The Internet of Things and cyber attacks.
- During the sessions, participants discussed policy aspects of cyber issues. They gained substantive knowledge, including various perspectives on the debate.
- Finally, during the simulation exercise, participants applied knowledge gained in the context which resembled a real-life policy process in terms of position of the main actors and negotiation dynamics.

This process was carefully prepared and implemented by the team, which was made up of content and process experts, including two senior diplomats who acted as diplomatic coaches.

## Programme

### Day 1 (Friday, 28th August)

09.15–10.00 Welcome coffee with CyberLab presentation: The future is now – the Internet of Things, 3D printing, and Bitcoin

10.00–10.15 Welcome remarks

- Ambassador Dhiravat Bhumichitr, Devawongse Varopakarn Institute of Foreign Affairs, Ministry of Foreign Affairs of Thailand
- Mr Bernhard Kelkes, Embassy of the Kingdom of the Netherlands, Bangkok
- Dr Jovan Kurbalija, DiploFoundation

10.15–11.30 **WHAT** are the main cyber diplomacy issues? (Mapping cyber challenges for modern diplomacy)

- Understanding how the Internet works and how Internet functionality impacts cyber diplomacy
  *By Vladimir Radunović, Director of Cybersecurity at DiploFoundation*
- Summarising the main cyber policy challenges for diplomats
  *By H.E. Dr Alex Sceberras Trigona, Special Envoy of the Prime Minister of Malta and Former Minister of Foreign Affairs of Malta*

11.30–11.45 Coffee break and CyberLab

11.45–12.30 Applicability of international law to cyber challenges
*By H.E. Dr Kriangsak Kittichaisaree, Ambassador, Ministry of Foreign Affairs of Thailand and Member of the International Law Commission of the United Nations*

12.30–13.30 Lunch break

13.30–14.30 **WHERE** is cyber diplomacy performed?

- Survey of the main cyber diplomacy processes and legal and policy instruments (including confidence-building measures and activities of UNGGE)
  *By Dr Jovan Kurbalija, Director of DiploFoundation and Head of the Geneva Internet Platform*
- Survey of regional cyber initiatives in the Asia-Pacific region
  *By Ms Jessica Woodall, Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute*
- Regional Digital Diplomacy
  *By Mr Sameer Sharma, Senior Advisor, Regional Office for Asia-Pacific, International Telecommunication Union*

14.30–15.00 **HOW**: Bringing together technical, diplomatic, and security aspects of digital policy

*By Mr Wanawit Ahkuputra, Deputy Executive Director, Electronic*

*Transactions Development Agency, Thailand & Member of the Government Advisory Council at ICANN*

15.00–15.30 Coffee break with CyberLab presentation: a peek into the Dark Web and tools for cyber attacks

15.30–16.15 **WHO** are the main actors in cyber diplomacy?

- Overview of the main actors
- Roles of stakeholders and models of public-private partnership

*By Mr Moedjiono Sardjoeni Matdullah, the Senior Advisor for International Relations and Digital Divide, Minister of Communication and Information Technology of the Republic of Indonesia*

16.15–18.15 Simulation exercise: Negotiating an international cyber declaration

- Skills and techniques for diplomatic negotiations
  *By Ambassador Kishan Rana, former Indian diplomat*
- Distribution of simulation roles
- Simulation exercise – first round

18.15–18.30 Summary of the day

20.00 Workshop dinner

## Day 2 (Saturday, 29th August)

09.00–10.30 Simulation exercise (continuation)

Participants complete the simulated negotiations, and discuss the lessons learned, during a debriefing session with experts

10.30–11.45 Coffee break and CyberLab

11.45–12.15 How can national governments address the challenges of cyber diplomacy?

- Benchmarking countries in cyber issues & the Global Cybersecurity Index
  *By Aaron Boyd, Chief Strategy Officer, ABI Research*
- National diplomatic services and their coverage of cyber issues (case studies)
  Panel discussion moderated by *Dr Jovan Kurbalija, Director of DiploFoundation and Head of the Geneva Internet Platform*

12.15–14.30 Presentation of certificates and lunch reception