A summary of interventions provided by ASPI's International Cyber Policy Centre during the OEWG informal intersessional meeting, New York, 2–4 December 2019

Session A: Cyber threat landscape: existing and emerging cyber threats

The first session on existing and emerging cyber threats generated a lot of views on the impact of sophisticated malware, AI-enabled cyberweapons and infringements of human rights online.

In its intervention, ASPI ICPC focused on the aspect of transparency and my proposition that a lack of transparency constitutes an increasing risk in how states cooperate among themselves and with (foreign-based) private actors.

What are the greatest risks to stability in cyberspace? Besides technological threats, I'd like to highlight how we—as the public—deal with cyber capabilities, activities and presumed threats, and how that might affect our collective exposure to threats emerging from ICTs.

As some of you know, between 2014 and 2017, ASPI ICPC published the *Cyber maturity in the Asia–Pacific Region* reports. Even though no update has yet been published, many trends remain largely the same as we described in December 2017. In fact, most trends have become more pertinent and visible:

- We see states developing and implementing national cybersecurity legislation, strategies and policies, often with very strong and explicit language, but more often than not without clear guidance about how laws and strategies are being implemented.
- We see more states developing military ICT capabilities in their defence forces or within their intelligence, police and law enforcement agencies.

The main issue might not be the existence of these capabilities. It's each state's sovereign right, after all. The collective challenge—and the main risk and threat—seems to be a general absence of transparency.

I'd like to highlight three elements of transparency that are linked to ICT threats and perceptions of those threats—past, current and future:

1. Greater transparency about the existence of a state's ICT capabilities
2. Greater transparency about operational policies that guide the activities of state agencies and state-sponsored entities
3. An element of transparency that we've observed while working on capacity-building efforts in Australia, Southeast Asia and the Pacific.

You'll be surprised how little awareness there is among many governments, civil society and industry about what's happening in cyberspace in the context of international peace and security, and how that's affecting or, fortunately, in many more cases, not affecting them.

This current lack of transparency about national security ICT incidents implies that we need more informed reporting and analyses to be available in the public domain.

Session B: Creating a cyberspace based on rules, laws and norms: how can stakeholders support governments?

Thank you, Mr Chair.

This is obviously not only a question for non-government organisations! Since this is an informal and consultative meeting, it would be worthwhile to learn how the member states, across the aisle, see the role of NGOs in implementing the 11 norms in their own state or elsewhere as part of their regional cyber-capacity-building efforts.

It would be quite insightful to see the commonalities. And I do acknowledge the efforts of the GFCE in this regard.

I'll briefly introduce an effort that we're currently implementing: it's a training-based effort together with think-tank colleagues from across the ASEAN region, who are also represented here. I hope to hear from them later today and tomorrow.

This is what we're currently investing in (two items) and what organisations like mine can do:

1. We're building a curriculum on the implementation of the 2015 UNGGE report. It's a training handbook very much inspired by formats and templates maintained by the UN's Integrated Training Services and inspired by the non-papers, explainer notes and working papers that member states and others have submitted, and are submitting, to the OEWG process.

   I want to highlight the bookmark that we produced. We have translated nicely crafted diplomatic language into catchphrases that normal people also understand:

   And, earlier this morning, Australia's UNGGE representative shared an explainer video explaining the UN framework for responsible state behaviour.

   Clip 1: The UN framework for responsible state behaviour in cyberspace

   Clip 2: The UN norms of responsible state behaviour explained

2. We're running, facilitating training sessions, workshops and dialogues. As implementation is eventually a national responsibility, we're currently organising a series of national training sessions across our region to encourage and enable the development of national road maps or national action plans on the implementation of the 11 norms.

Such a Track 2.0 facilitated training and capacity-building effort enables a dialogue in a transparent and confidential setting, in line with what my colleague from ISIS Malaysia just highlighted.

One take-away from the work we started earlier this year?

As the rules and norms are reflective of common state practice, lots of things that amount to implementation are already taking place. We're not starting from scratch, but we haven't framed lots of work in the context of the UN norms. And this is meant as an encouragement!

Only last week, during a workshop hosted by Vietnam, we received a presentation from one ASEAN member state clearly articulating how its national cyber law is aligned with the 11 norms from the UNGGE report—quite unique, I dare to say. Thanks to a dialogue facilitated by us, other participating states recognised that they hadn't sufficiently consulted the internet tech community, critical infrastructure providers and civil society, and took that back to their capitals as an action item.

We're very happy to share our lessons learned, but I'd also like to extend an invitation to all those represented here, our colleagues on this side of the room and the OEWG member states, to co-develop materials tailored to regional and national contexts that at the same time reflect the global consensus.

Session D: Confidence building measures and capacity building: confidence-building between states and between states and the private sector

ASPI recalled the collective work with eight Track 2.0 think tank organisations from across ASEAN on cyber confidence-building measures that resulted in the Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN Region.

Session E: Confidence-building measures and capacity building: engaging all stakeholders to enhance capacity-building efforts

Thank you, Mr David Koh, chair of this intersessional meeting, Mr Jurg Lauber, chair of the OEWG and thank you to UNODA for extending the opportunity to provide this first scene-setter about capacity building.

For those of you who don't know me, my name is Bart Hogeveen and I'm working at the International Cyber Policy Centre at the Australian Strategic Policy Institute, where I'm managing a very interesting ('cool' is the word I'd use) but modest cyber capacity-building program.

A scene-setter about cyber capacity building in ICTs in the context of international security. But, in fact, the question I'd like to pose to all of you here is: what do we actually mean by cyber capacity-building?

It appears to me that 'capacity building' is too frequently the simple diplomatic, uncontroversial answer to yet another wicked problem that we're confronted with. If it only were that easy.

Coordinated cyber capacity-building has been on our collective agenda for the past 10 years at least. I can simply refer to the consecutive substantial reports of the UNGGE and also to the conclusions of the 2015 Global Conference on Cyber Space in The Hague.

Now, if you look at what capacities, capabilities and resources we've been collectively able to deploy, and what we've been able to strengthen and sustain, in industrialised economies as much as in developing nations and states that only recently connected to the internet, I'd argue that results are far from optimal.

Yes, the internet technical community and the CERT community have been phenomenal at building, and training CSIRTs, network operator groups, internet exchange points and so on.

Yes, our colleagues in law enforcement and policing have been great at training and equipping police cybercrime units across the globe.

But, Mr Chairman, those efforts run the risk of becoming 'white elephants' when they aren't accompanied by comparable investments in potentially more soft and sensitive issues to do with laws, strategy and policy; resilient institutional arrangements with proper checks, balances and oversight; and a good understanding of what a society needs and expects.

And here's a problem: you can't see, approach and program capacity-building solely from an international policy angle, nor from a solely technical angle, human rights angle or siloed cybersecurity angle.

We need a far more comprehensive approach to cyber capacity-building that indeed brings technical expertise together with domestic and international cyber policy expertise and—very much so—development expertise.

And I'd like to stress the last of those: development expertise.

Because, Mr Chairman, what we see is that there's a lack of coordination between donors. This is not an unknown challenge in international aid, and I'm under no illusion that it will be resolved here, but that doesn't mean that we shouldn't do our best to at least prevent a duplication of efforts.

There's an issue with a substantial scarcity of resources (that are *de facto* available): human resources, sustainable financial resources and appropriate skill sets.

There's an issue with appreciating a nation's absorption capacity, a need for local ownership and a need for capacity-building programming that's tailored to local contexts.

I doubt that the terms I've just used have been part of the First Committee Disarmament and International Peace and Security meetings, and that's exactly where the shoe pinches, in my opinion.

Mr Chairman, let me conclude with a call for action on the front of cyber capacity-building in ICTs in the context of international peace and security:

- The international cybersecurity capacity-building effort needs a dedicated, specialised, operational and donor-neutral international core team of experts.
- We need a core team of experts that can initiate, program, design, resource, manage, execute and evaluate cyber capacity-building efforts in partnership with a host nation.
- We need a core team of experts that can consult short-term technical assistance that resides in public, private and non-for-profit organisations; for instance, from agencies represented here today and from members of, for example, the Global Forum on Cyber Expertise.

In one of my earlier interventions, I referred to the UN's Integrated Training Services (within the Department of Peacekeeping Operations) as an example, and I can also refer to the International Security Sector Advisory Team working out of Geneva as an example of such capacity-building resources in other areas of international peace and security.

These are examples of entities, independent of donor preferences, that focus purely on the transfer of knowledge, on enhancing national skills and organisational skill sets and on creating an enabling environment for a locally owned development process on sensitive topics involving security. To answer the question with which I started: in my mind, this is what capacity building is in essence about.

To conclude: we don't need more talking *about* capacity building. We need a far greater effort on doing it—doing it professionally, comprehensively and in closer partnership with local partners.

Mr Chairman, thank you for your attention.