

08 June 2015

The third meeting of the Sino-European Cyber Dialogue (SECD) was convened on 20-21 April 2015 in The Hague, the Netherlands. The meeting was hosted by the [China Institutes of Contemporary International Relations](#) (CICIR) and [The Hague Centre for Strategic Studies](#). SECD is supported by the Chinese government, a number of European governments as well as the [European External Action Service](#).

The Dialogue followed on the heels of the [Global Conference on Cyberspace 2015](#) and fit the conference's emphasis on building trust and cooperation. "This Dialogue represents the only true track 2 format for communicating cyber policy issues between China and Europe," said Standing Rapporteur Alexander Klimburg. "In itself it is a critical tool towards building confidence and stability in cyberspace."

Overall, thirty-eight participants and a number of observers attended the third meeting of SECD. Nine European countries were represented, as well as two EU institutions, with particular emphasis on foreign ministry cyber policy coordinators. As in [previous discussions](#) delegates concentrated on two broad topics: overall issues within international cybersecurity and views on the development of Internet governance.

Within the first topic, there was discussion on particular aspects of state behavior in cyberspace, and how these can negatively affect the strategic stability between nations. The malicious use of ICTs, especially against critical infrastructure, was seen as an area of mutual concern. Delegates also discussed issues arising from non-state activity in cyberspace. There was general agreement that at the operational level it was necessary to build trust between technical actors (such as CERTs) as a basis of further cooperation. Confidence building measures, both at the bilateral, regional, and international levels were seen as being the most promising instruments for political agreements. The specifics on the application of international law to cyberspace were discussed, both sides exchanged opinions based on their own key concerns. It was agreed that issues below the threshold of armed conflict could be prioritized for discussion. The prospect of a potential "Helsinki Process for Cyberspace" was debated, and would need to address issues both below and above the threshold of armed conflict, and not be limited to security baskets.

On Internet governance-related issues, there was full agreement that the multistakeholder approach would remain the principle governance model. There was however hopes that in other aspects related to Internet governance there would be a better coordination between issues of "more multistakeholder" and issues of "more multilateral" (intergovernmental) concern. Both sides stressed that the continuing globalization of Internet governance, including the transition of the IANA function, would be a key test. Both sides agreed that much more attention needed to be paid to the role of the developing world in accessing the Internet and participating in its governance. Capacity development programs towards this end were discussed and widely considered to be to the benefit of all actors. The "fragmentation" of the Internet was considered to be an undesirable option.

In conclusion, both sides agreed that it could be worthwhile to examine further modes of cooperation between Europe and China on international cybersecurity and related issues.