ISA Roundtable 2021: Cyber Dimensions of Chinese Politics
6-8 am MST, April 9, 2021

Sebastian Harnisch, Heidelberg University

Following the so-called Facebook and Twitter revolutions in the Arab World in 2010 and 2011, expectations ran high that the emerging microblogging sphere in China might facilitate the empowerment of local civil society and eventually initiate a political transformation. However, case studies and empirical analyses of the Chinese Internet lead to a more complex picture – one that highlights instead the symbiotic relationship between state and society. This roundtable looks at the cyber dimension of Chinese politics from three distinct perspectives: 1. It starts with an in-depth analysis of the most recent trends in online deliberation, the steering of public opinion, as well as the possibilities and limits of the formation of a civil online sphere via Weibo/WeChat. 2. In this vein, it also assesses the role of big data in the algorithm-based monitoring and control of society and takes a closer look at the impact of "deep learning" on the making of Chinese politics. It continues by putting these findings into the broader context of cyber conflict behavior in authoritarian versus democratic system settings. 3. It finally concludes with a theory-guided evaluation of AI innovation and the future of China's "smart city" and "smart government" solutions, linking online and offline governance dimensions).

Speaking Notes:

Thank you very much, Nele for bringing us together on this timely and important topic. In the paper, entitled Cyber sovereignty and China's cyber self-assertion: a role theoretical explanation and some empirical evidence, I make three claims:

First, foreign policy role theory can and should be used fruitfully to examine China's assertion of cyber sovereignty and Cyber superpower status. Specifically, self-assertion is conceptualized as institutionalized superimposition of one's own expectations of a role over others, the contestation of a given international (liberal) order, including self-elevation over others by denigrating them and the altercasting of the United States as the only appropriate peer in a "new type of great power relationship".

Second, in the empirical chapters I trace the CPC institutional self-assertion under Chairman Xi through the centralization and hardening of China's cyber sovereignty domestically. In turn, the paper analyzes China's promotion of Cyber sovereignty in the UN, SCO and BRI context and describes how the CPC leadership grew increasingly bold, especially after 2015, to reverse the thrust in its asymmetrical interdependence with the West: first by launching administrative reforms, i.e.

Cyberspace Administration of China, the Cyber Security law and the Strategic Support Force, and second by fusing military and civilian as well as private and state-led enterprises to outcompete the United States in leading IT technologies, including, blockchain, electronic payment and currency priviosn, AI etc. Notably, China has used bilateral accords temporarily, such as the XI-Obama agreement on economic espionage in 2015 to protect its growing IT sectors from economic sanctions, but has not yet in comparison to Russia led multilateral initiatives in the UN context to establish an alternative international cyber order.

Third, the paper employs a new data compiled at Heidelberg University, which focuses on technical and political attribution of cyber operations. Examining China's cyber operations, several patterns become visible: political and disruptive operations are primarily targeted towards domestic oppositional, diaspora groups or other claimants in the SSC, Taiwan being the prime target. Economically, Chinese operation focus on the US, governmental, academic and commercial entities, mainly for technology and/or trade gains. In comparison to Russia operation, disinformation plays a smaller but growing role, i.e. COIVD-19, Hongkong. Overall, an increase in Chinese extractive operations intensity is detectable during the Trump administration, with the Microsoft exchange hack still under investigation.

In conclusion, the paper argues that China cyber self-assertion is neither a result of growing power or less benign purpose under Xi Jinping. China's attempt reassert itself as a Sovereign Cyber Superpower stems from its position as an ascending autocratic power in a still liberal international cyber order with the United States as a dominant offensive cyber power, especially under the Trump administration. Thus, from a relational perspective, China's attempt may well fail partially or totally as other actor's the United States in particular, reassert themselves too or delegitimize China's claim to shape a "common cyber future for mankind". Super power roles, as social structures, do not belong to an actor alone. Instead, leading roles must be earned if they are based on legitimate claims of authority.