Marshals Over Markets: China Tightens Cybersecurity

Lance Noble
lnoble@gavekal.com

Arthur Kroeber
akroeber@gavekal.com

Summary

China has recently moved to tighten regulations on cyberspace, for a mix of national security, social control and industrial policy reasons. These rules could have major effects on businesses and China's economy.

China is not alone: most other major economies are strengthening rules to protect online data privacy, safeguard critical technology infrastructure, and regulate cross-border data flows. But China's efforts are far more expansive, and raise more serious concerns. Its definition of national security is broad and encompasses economic issues as well as defense. Much of the new regulatory framework seems designed to create powerful domestic technology firms. And the requirements for local data storage and limits on cross-border data transfer are the most stringent in the world.

Our principal findings are:

1. **Three competing agendas drive China's cyber-regulation.** These are a **control** agenda focused on national security and social control; an **industrial policy** agenda aimed at increasing Chinese tech firms' share of domestic and global markets; and a **governance** agenda driven by the need to respond to rising citizen pressure for online data privacy.
2. **The rules are not set in stone, and there is space for successful lobbying by companies.** China needs a vibrant digital economy connected to global innovation systems. Regulators, trying to balance security and economic interests, are open to constructive input.
3. **China will become one of the world's three main cyber-regulators (along with the US and European Union), and companies must adapt to a fragmented global cybersecurity regime.** The need to maintain separate data centers and product sets for different jurisdictions will raise costs and disadvantage smaller firms.
4. **The biggest immediate problem is uncertainty about the rules on collection, storage and cross-border flows of data.** China's data rules are by far the most restrictive in the world. But exactly how these rules will be enforced is still up for negotiation between regulators and business. Some foreign companies have put on hold plans for R&D centers and other facilities requiring seamless global connectivity.
5. **Security certifications for ICT products are a confusing mess.** ICT products sold in China must meet new security standards. But it is unclear who will enforce these standards, and how they will interact with existing security standards in place since 2007.
6. **Intellectual property protection may get harder.** With strict local data storage rules, and an inability to use the most advanced encryption tools, companies face a higher risk of data and IP leakage.

Contents

The authors

Lance Noble is senior thematic policy analyst at Gavekal Dragonomics.

Arthur Kroeber is founder and head of research of Gavekal Dragonomics.

DeepChina reports

Published 3-5 times a year, DeepChina reports are in-depth investigations of key topics in China's economy, politics and society. They are written by Gavekal Dragonomics staff and our network of expert external contributors.

© Gavekal Ltd. Redistribution prohibited without prior consent. This report has been prepared by Gavekal mainly for distribution to market professionals and institutional investors. It should not be considered as investment advice or a recommendation to purchase any particular security, strategy or investment product. References to specific securities and issuers are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities. Information contained herein has been obtained from sources believed to be reliable, but not guaranteed.