GLOBAL 21.09.2020 | Dani Rodrik

The coming global technology fracture

Today's international trade regime was not designed for a world of data, software and AI. It needs drastic change

The international trade regime we now have, expressed in the rules of the World Trade Organization and other agreements, is not of this world. It was designed for a world of cars, steel and textiles, not one of data, software and artificial intelligence. Already under severe pressure from China's rise and the backlash against hyper-globalisation, it is utterly inadequate to face the three main challenges these new technologies pose.

First, there is geopolitics and national security. Digital technologies allow foreign powers to hack industrial networks, conduct cyber-espionage and manipulate social media. Russia has been accused of interfering in elections in the United States and other Western countries through fake news sites and the manipulation of social media. The US government has cracked down on the Chinese giant Huawei because of fears that the company's links to the Chinese government make its telecoms equipment a security threat.

Second, there are concerns about individual privacy. Internet platforms are able to collect huge amounts of data on what people do online and off, and some countries have stricter rules than others to regulate what they can do with it. The European Union, for example, has enacted fines for companies that fail to protect the EU residents' data.

Third, there is economics. New technologies give a competitive edge to large companies that can accumulate enormous global market power. Economies of scale and scope and network effects produce winner-take-all outcomes, and mercantilist policies and other government practices can result in some firms having what looks like an unfair advantage. For example, state surveillance has allowed Chinese firms to accumulate huge amounts of data, which in turn has enabled them to corner the global facial recognition market.

The need for regulatory diversity

A common response to these challenges is to call for greater international coordination and global rules. Transnational regulatory cooperation and anti-trust policies could produce new standards and enforcement mechanisms. Even where a truly global approach is not possible – because authoritarian and democratic countries have deep disagreements about privacy, for example – it is still possible for democracies to cooperate among themselves and develop joint rules.

There is little evidence that Huawei has engaged in spying on behalf of the Chinese government. But that does not mean that it will not do so in the future.

The benefits of common rules are clear. In their absence, practices such as data localisation, local cloud requirements, and discrimination in favour of national champions create economic inefficiencies insofar as they segment national markets. They reduce the gains from trade and prevent companies from reaping the benefits of scale. And governments face the constant threat that their regulations will be undermined by companies operating from jurisdictions with laxer rules.

But in a world where countries have different preferences, global rules – even when they are feasible – are inefficient in a broader sense. Any global order must balance the gains from trade (maximised when regulations are harmonized) against the gains from regulatory diversity (maximised when each national government is entirely free to do what it wants). If hyper-globalisation has already proved brittle, it is in part because policymakers prioritised the gains from trade over the benefits of regulatory diversity. This mistake should not be repeated with new technologies.

The Huawei case

In fact, the principles that should guide our thinking on new technologies are no different from those for traditional domains. Countries may devise their own regulatory standards and define their own national security requirements. They may do what is required to defend these standards and their national security, including through trade and investment restrictions. But they have no right to internationalise their standards and try to impose their regulations on other countries.

Consider how these principles would apply to Huawei. The US government has prevented Huawei from acquiring American companies,

restricted its operations in the US, launched legal proceedings against its senior management, pressured foreign governments not to work with it, and, most recently, banned US companies from selling chips to Huawei's supply chain anywhere in the world.

There is little evidence that Huawei has engaged in spying on behalf of the Chinese government. But that does not mean that it will not do so in the future. Western technical experts who have examined Huawei's code have been unable to rule out the possibility. The opacity of corporate practices in China could well obscure Huawei's links to the Chinese government.

The Huawei case is a harbinger of a world in which national security, privacy, and economics will interact in complicated ways.

Under these circumstances, there is a plausible national security argument for the US – or any other country – to restrict Huawei's operations within its own borders. Other countries, including China, are not in a position to second-guess this decision.

The US crackdown lacks legitimacy

The export ban on US companies, however, is harder to justify on national security grounds than the ban on Huawei's US-based operations. If Huawei's operations in third countries pose a security risk to those countries, their governments are in the best position to assess the risks and decide whether a shutdown is appropriate.

Moreover, the US ban confronts other countries with severe economic repercussions. It creates significant adverse effects for national telecoms companies like BT, Deutsche Telekom, Swisscom and others in no fewer than 170 countries that rely on Huawei's kits and hardware. Perhaps worst hit are poor countries in Africa that are overwhelmingly dependent on the company's cheaper equipment.

In short, the US is free to close its market to Huawei. But US efforts to internationalise its domestic crackdown lack legitimacy.

The Huawei case is a harbinger of a world in which national security, privacy, and economics will interact in complicated ways. Global governance and multilateralism will often fail, for both good and bad reasons. The best we can expect is a regulatory patchwork, based on clear ground rules that help empower countries to pursue their core national interests without exporting their problems to others. Either we design this patchwork ourselves, or we will end up, willy-nilly, with a messy, less

efficient and more dangerous version.

(c) Project Syndicate



Dani Rodrik
Cambridge

Dr Dani Rodrik teaches International Political Economy at the John F. Kennedy School of Government of Harvard University. He is the author of *The Globalization Paradox: Democracy and the Future of the World Economy* und *Economics Rules: The Rights and Wrongs of the Dismal Science*.