Australia-China Relations Institute
澳中关系研究院

Opinion

Cyberspace: The new battlefield of US-China competition

Marina Zhang
December 9 2022

Note: This article appeared in *The National Interest* on December 9 2022.

There are 2.8 billion active monthly users on Facebook, 1.3 billion on WeChat, and 1 billion on TikTok. During the Covid-19 pandemic, the netizen population grew rapidly when people and businesses migrated online, resulting in a process of digital transformation. As a result, organisations and infrastructure—from electricity grids, telecommunications networks, and police departments, to banks, hospitals, and schools—are accumulating vast amounts of data to provide value to users.

While digital technology enables connectivity, convenience, and efficiency, the pervasive use of data collection and analytics in the social, financial, industrial, and military sectors has exposed the vulnerability of cyberspace in ways never previously experienced. Cybersecurity threats— whether from an individual, an organisation, or a global syndicate—have the potential to damage private and public interests, destabilise the international order and endanger world peace.

The international community has yet to reach a global consensus about a digital order that can deal with issues in this increasingly complex space. Without such a consensus governing cyberspace, a global digital disorder will soon arrive.

An international digital disorder

When discussing potential disorder as a result of competition between two nuclear-powered states, Henry Kissinger said, 'Neither side would use its weapons of mass destruction because the adversary was always able to inflict an unacceptable level of destruction in retaliation.' Kissinger's assumption was that states know who their adversaries are, and can even have signals of potential attacks and prepare for them. Therefore, a strategy of deterrence was effective.

Unfortunately, this calculation doesn't work in cyberspace anymore. Cyberspace largely exists on the internet. Except in dedicated networks, most users and smart devices interact and exchange information freely in cyberspace.

An underground hacker or syndicate that illicitly accesses these networks can cause catastrophic consequences. They can access the cyber domains of governments or businesses to disable and potentially destroy critical national infrastructure or networks. Others can simply be motivated by money, stealing data to trade on the black market or demanding a ransom. For example, in Australia, a cyberattack on the telecommunications company Optus and a ransomware attack on Medibank compromised the personal data of almost 20 million people, including their names, phone numbers, government-issued IDs, and other

sensitive information. The real challenge is that it is very often almost impossible to identify the hackers or attribute them to any sovereign state.

Amid heightened geopolitical tensions, cyberattacks can also be launched by states, which can threaten the national security of their adversaries and inflict costs equivalent to conventional war.

While cyberspace is assuming enormous importance, it is becoming a less orderly territory, where no clear, commonly agreed upon international order governs the behavior of actors—which include governments, private organisations, individuals, and, increasingly, artificial intelligence-empowered devices. In the absence of such an international digital order, actors will continue to follow their own rules and norms, and the likely outcome is chaos in cyberspace.

Cyber-sovereignty

Of all the issues related to the international digital order, cyberspace sovereignty stands out, even though the concept is vaguely defined. Currently, the international consensus is that cyber sovereignty should follow the rules of sovereignty outlined in the United Nations Charter.

Since the establishment of the UN, there has been a consensus that sovereign autonomy is the basis for international law. Because of the open, multi-layered, anonymous, and borderless nature of cyberspace, it is difficult to distinguish between domestic and international breaches of law. For this reason, the UN's sovereignty rules cannot be easily applied to cyberspace. If cyber sovereignty exists independently in the online world, does cyber sovereignty belong to each country? Or is there—or should there be—a supra-national, supra-sovereign global body that governs cyber actors and their activities?

The challenge of building an international consensus on cyber sovereignty is that different countries have different perspectives and different needs. For example, China has long promoted international rules to guarantee cyberspace sovereignty. Beijing's argument is that when the cyber sovereignty of a state is attacked, its network systems can be invaded and networked data will be compromised. In such situations, without a common understanding of the jurisdictional boundaries of cyber sovereignty, it is difficult to punish the attacker or counteract the invasion.

In the first decade of the twenty-first century, the United States began promoting a 'network super-sovereignty' concept, arguing that sovereign states have little sovereign jurisdiction over the internet, as it should belong to the global population and be a platform for freedom and democracy. The essence of this theory is to oppose cyberspace sovereignty by promoting cyberspace hegemony, which has laid the foundation for the framework of US internet policy.

In response to recent calls to build a co-governance framework, the United States has shifted its internet policy away from advocating openness and freedom and pursued global 'multi-stakeholder' governance, which has received support from large tech firms and countries with significant cyber capabilities. However, internet users and their representatives in countries without dominant cyber capabilities have little opportunity to participate in this framework.

Data security and national security

Regulations and rules for data security, especially in cross-border data flows, are another imperative for building an international digital order.

Due to the dual-use nature of digital technologies such as artificial intelligence (AI) and quantum computing, the boundaries between national economic interests and security interests have blurred, which has led sovereign states, especially the United States and China, to consciously or unconsciously regard data security as synonymous with national security. Indeed, with the advent of big data analytics empowered by AI algorithms, the importance of personal data to national security is increasing, and data can be used or manipulated by one country to achieve its geopolitical goals against others. If a country's citizens' private data, such as their political affiliations, medical records, biometric data, or even data about their physical movements, is captured by hackers or hostile states, that data can be analysed to create a security threat to

the host country. It was for this reason that the Chinese government investigated and subsequently punished the ride-hailing company Didi after its initial public offering on the Nasdaq.

In contrast to the limited nature of traditional strategic resources such as land, oil, and minerals, data has the characteristic of non-exclusiveness, or network effects—the more data is used, the more value it has. At the individual level, data can be personal property and can carry the imputation of privacy. At the economic level, data can be a factor of productivity and a competitive advantage for an enterprise. And at the state level, data can be a strategic resource and can carry significant security value. Therefore, data can be sold for profit; there are black markets for trading stolen data through specialised hidden websites, creating yet another layer of complexity in identifying data hackers.

While most governments and organisations have implemented technologies to safeguard their data security, there are two main dynamics that can expose their vulnerabilities to potential cyber threats.

First, the prevalence of cloud computing, which enables organisations to outsource all or part of their data management to third-party companies, a field that is currently dominated by several leading firms in the United States and China. The top five—Amazon, Microsoft, Alibaba, Google, and Huawei—accounted for over 80 percent of the global market in 2021. Second, many organisations and even governments have to rely on third-party vendors—usually involving multiple suppliers—to build their cyber capabilities, which can leave the 'back door' open for a so-called 'supply-chain attack.' Therefore, many governments and organisations have started to adopt a 'zero-trust framework' in their networks. It was for this reason that China's vendors of 5G or web camera equipment have been suspended in network systems in the United States and allied countries.

The reality is that the digital economy is replacing the commodity trade and traditional financial activities as the main driver of globalisation, which is reflected in the growing trade of data-oriented services. There is an urgent need to build a global consensus on the cross-border data trade, including financial services data, governing data acquisition, processing, storage, and transfer across borders.

Great power rivalry in cyberspace

Great power competition in cyberspace between the United States and China carries enormous strategic significance for both countries. Washington and Beijing's core objective in this competition is to use supremacy in cyber capabilities to their geopolitical advantage. Underlying cyber capability is a country's accumulated technological power in semiconductor chips, computer operating systems, and electronic design automation tools, which lay the ground for high-performing computing, AI, and next-generation internet and mobile communication networks.

For this reason, the escalation of the great power rivalry between America and China, from trade war to tech war, has centered on competition in those advanced foundational technologies, as they have become critical resources for national sovereignty, economic development, and national security.

This competition is not just about technical standardisation—it has also shifted to the political arena, where both parties are fighting over rules and regulations for the management of data transfers and data storage. The US strategy to contain China's advancement in semiconductors is a conspicuous manifestation of this competition.

China's growing cyber capabilities have allowed it to increase its influence in setting standards relevant to the design and operation of the future internet, and to promote an international digital order, which is interpreted by the West as serving China's geopolitical goals. The US government has developed a grand strategy based on 'digital realpolitik,' with a primary objective of advancing US cyber dominance and limiting its main digital adversary—China.

Great power competition in cyberspace is that it has increased the danger of decoupling in technological systems, and even in cyberspace itself, unless a consensus can be reached to build an international digital order.

A new kind of digital divide

When we talked about the digital divide a decade ago, we referred to the gap between rich countries, where people had access to the internet through networked computers and smart devices, and poor countries, where people had less access. With the rapid penetration of low-cost smartphones (largely made by Chinese producers) in underdeveloped countries, this digital divide is shrinking. However, there has emerged another digital divide defined by cyber capability: countries with advanced cyber capabilities and countries with fewer capabilities.

The internet is an open network woven together by globally standardised data communication protocols and managed from the bottom up. Billions of users and digital devices interact, generating massive amounts of data. In other words, the internet is highly decentralised, and every user is equal in generating data.

In reality, however, not every actor is equal in cyberspace. Individuals, organisations, and governments that possess more advanced cyber capabilities make the rules, not just in technical standards but also in institutional regulations. Because of high switching costs, organisations and states enjoy a pre-emptive technology monopoly built upon path dependence if they are first or early movers in cyberspace.

For example, in 2021, the top five US-based tech giants—Amazon, Alphabet, Microsoft, Apple, and Meta–Facebook—and the top five China-based giants—Huawei, ByteDance, Alibaba+Ant, Tencent, and Baidu—collectively controlled over 50 percent of online traffic and dominated the world's digital infrastructure. In 2020, these five American tech giants invested over $120 billion in research and design, and the top five Chinese giants invested over $60 billion, accounting for 18 percent and 10 percent, respectively, of their countries' total R&D expenditure. These figures are on par with or greater than the R&D investment of many industrial countries. Thus, these nonstate actors play a critical role in the standardisation and shaping of the de facto digital order.

The advantages of these big firms are compounded by the fact that, in the tech world, innovation in technology and business models often outpaces the development of rules and regulations—and, indeed, the comprehension of policymakers. For this reason, the balance of power between states divided by cyber capabilities is inherently asymmetrical: countries with advanced cyber capabilities will dominate the technological frontier and the international digital order.

Does this asymmetry of power mean that countries with fewer cyber capabilities or fewer large tech firms must subordinate themselves to high-tech societies such as the United States and China in building an international digital order?

Implications for the rest of us

The road to an international digital order may be long and uncertain, but no meaningful progress can be made if the discourse about it is confined to the two great powers in cyberspace. Their interests may not be aligned with the rest of the world.

However, constrained by their limited cyber capabilities, most countries currently have little participation in, or influence over, this discourse.

In contrast to a world order that is determined by superpowers, data is globally distributed, meaning that any digital order should be inclusive of state and non-state actors, both large and small. Ultimately, we are all data generators and should benefit from the value derived from that data. Cyberspace, as a new arena for global activities, requires that all members, regardless of their strength, have a say in the making of an international digital order.

Dr Marina Zhang is Associate Professor – Research at the Australia-China Relations Institute, University of Technology Sydney.