Economics & Security: Key National Interests for Discussion

Author Naoyuki Haraoka

By Naoyuki Haraoka

Geopolitical Uncertainty Influencing Global Economy

The IMF Economic Outlook published in October 2019 predicts world economic growth for 2019 to be 3.0% and for 2020 to be 3.4%. However, there are big risks such as trade and currency wars, cumulating government debt, and deep security tensions. Security risks include an unstable Middle East, uncertainty on the Korean Peninsula, China's assertive foreign policy and an unpredictable US foreign policy, and growing cyber risks, as well as weakening global governance. Before the global financial crisis in 2008, an emerging market could be defined as any country where politics mattered to the market as much as economic fundamentals, while the G7 countries provided a much more stable and predictable political landscape. But since that crisis, politics has started to affect economic and market performance more directly, even among those wealthy countries. The rising income gap between the wealthy and the poor has been the background to increasing discontent among ordinary voters, which has prompted moves against globalization and the free flow of goods and services, as these can trigger increases in unemployment or poverty among non-skilled workers. The move toward nationalism has destabilized politics even in developed nations, and has also brought an end to US-led global governance with Washington's withdrawal from a number of international arrangements for rule-making, such as the Trans-Pacific Partnership (TPP) or Paris Agreement on global climate change. Without solid leadership in global governance, geopolitical instability becomes inevitable. Thus, today it is not economics but geopolitics that is the main driver of global economic uncertainty.

Economics & Security Need to Be Discussed Together

It is noteworthy that in this growing geopolitical uncertainty digital technology plays a key role. Digital technology creates huge business opportunities, but it also brings malicious factors such as growing cyber risks and threats to national security through trade and investment in sensitive technologies. Digital technology, including quantum computing, machine learning and 5G, has transformed most domains of human activity, such as people's interactions or exchange of information in business management, and also in defense and security. The digital economy and society has made countries vulnerable to cyberattacks by both state and non-state actors. We now need to reflect on how to maximize the benefits of digital technology in terms of economics, while paying proper attention to those technologies' implications for national security, though economics and security have been viewed largely as separate issues of national interest in the past. Economics and security should now be discussed together as inseparable issues.

In particular, at this moment, the major developed nations seem increasingly willing to advocate for their economic and security interests unilaterally. This has enhanced the need to discuss both issues together to create common rules. In this context, we should bear in mind that security will be key to achieving prosperity, and prosperity will in turn help pay for security. If social disharmony brought about by rising income disparities increases economic and security risks, then it becomes imperative to ensure social harmony to achieve security and prosperity.

This means that the silo approach to studying economics and security issues completely independently is now obsolete. Prosperity, security and social harmony are the important components of national interest. All three matter, and they need to be discussed together in order to mitigate the risks they face.

Tackling Risks to National Interests

Countries exposed to security risks need to balance possible solutions against their strong economic interests. Mitigations of security risks could be achieved by supporting market systems and people-to-people connections through migration or research collaboration rather than confrontation, as well as strengthened domestic defense and security governance systems. In this regard, globalization would not be contradictory to national security but rather promote it. Interdependence among nations through cooperation could lead to mitigation of security risks.

While defense and security are public goods to be provided by governments, risk mitigation can be provided by not only governments but also business and civil society. Governments are mainly responsible for creating incentives for the private sector to mitigate risks. Laws and governance institutions supported by effective enforcement would help business and civil society in contributing to risk mitigation over time.

A scenario approach would be useful for such risk mitigation and management, since risks are affected by a wide range of actors, such

as domestic politics, international relations in hot spots like the Korean Peninsula or the Middle East, and technological change and the impact of data and digitalization. There could be a number of scenarios depending upon those variables. Such scenario-making would enable policy practitioners or private businesses engaged in risk mitigation to have an analytical framework to eliminate arbitrary thinking and achieve a logical and strategic approach to a complex issue.

Strategic thinking is very useful in considering foreign direct investment (FDI) in digital and telecommunications infrastructure. First, we need to identify the risk of a cyberattack by malicious states or companies which could disable key telecommunications infrastructure. Then we should prepare strong defenses in firms and organizations against cyberattacks, endorsed by enforcement of strong laws. We should build up a much less oligopolistic market, since the risk of becoming a victim of cyberattacks will be lowered with more players in the market. In building up digital networks, creating more competitive and diverse market structures with less concentration of a small number of large actors would lead to better risk mitigation, rather than discussing only the issue of foreign ownership of the companies involved in building up these networks' infrastructures.

Another risk exists in data. There will be concerns about firms' susceptibility to theft of personal data by cyberattacks. This risk could be logically and strategically reduced by cyber defenses strengthened and supported by the enforcement of strong laws on the protection of privacy and by corporate transparency.

In order to meet the challenge of the risks produced by complex new digital technologies, first it would be important to assess these risks clearly and identify exactly what they are and try to use all kinds of standard knowledge to mitigate them. This must be done creatively and strategically. Most importantly, we will need international collaboration rather than confrontation. New technology has created the need for a new international cooperation order rather than confrontation among nations. So we will need new global governance for risk mitigation related to digital technology.

Japanese Leadership Needed to Achieve New International Order

To realize a world in which the United States and China work together on practical and mutually beneficial steps to address their tech cold war, Japan would need to play a critical leading role. Japan could boost cooperation with China and the US by taking advantage of its unique position and providing each of them with incentives for cooperation in areas where their national interests coincide. Japan could at the same time work with like-minded nations, such as Germany, Canada, France and the United Kingdom, to defend and support existing international institutions and play a leadership role in global rule-making for trade, data transfer, and innovation policies. This could be possible in light of its achievements in having realized the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) despite the withdrawal of the US from the TPP in January 2017. Whereas the CPTPP was signed by 11 countries in December 2018 and is open to the US, the Regional Comprehensive Economic Partnership (RCEP), another Asia-Pacific regional FTA, was agreed by 15 countries in November 2019 for signing into law in 2020 and is open to India. These mega-regional FTAs could lead to the foundation of a new multipolar global order.

In addition, APEC, a wider regional group of Asia-Pacific nations including CPTPP and RCEP member nations, could be a good place for ministers and officials to discuss economics and security together to deliver prosperity, security and social well-being simultaneously. APEC also has an advantage in its informal connections with business and thus the private sector could express their views and concerns regarding risks to their national interests related to economics and security. Although APEC's discussions may have no binding effects, such informal exchanges of views on economic and security policies could result in reasonable peer review pressure upon the member nations. Japan, a member of all these three groups – the CPTPP, RCEP and APEC – could contribute effectively to policy discussions in APEC to initiate a new global order to help resolve the issues of economics and security together.

Finally, as for cyber security, Japan could continue to work on a cyber coordination and monitoring center. This would be useful in encouraging FDI in research and development which has been declining during these days of the US-China tech cold war.

A world without leadership that people can trust would be disastrous, especially in the light of digital technology. New technology progresses rapidly. We may not have much time to create a new order that people can count on. JS

Naoyuki Haraoka is editor-in-chief of *Japan SPOTLIGHT* & executive managing director of the Japan Economic Foundation (JEF).