National Security and Economic Resilience Roundtable
Led by Lord Sedwill

On 18 March 2021, former Cabinet Secretary and National Security Adviser Lord Sedwill chaired a joint RUSI and Cabinet Office roundtable with experts from academia, the private sector and the public sector to discuss national security and economic resilience ahead of the 2021 G7 Summit. Discussion centered around the security risks generated by emerging technologies and increasing economic interdependence between G7 countries and China. Themes included: the globalisation of technology and supply chain resilience; cyber resilience; strategic competition and sovereign capability; the role of research and development in economic resilience; the strategic role of the G7.

This summary collates the main points provided by participants during these sessions. They reflect the views of individual attendees, not RUSI or any other organisations. This is not a published RUSI product and should not be treated as such.


The coronavirus pandemic has put economic resilience at the front and centre of the political agenda. However, as the chair noted, the underlying challenges to economic resilience are much broader and longstanding than the physical supply of medical equipment or other essential goods. The chair highlighted several forms of risk that could impact the economic resilience of the G7 members:

- **Economic risk**: There are underlying market gaps across a range of sectors beyond those that have hit the headlines over the last 12 months. Most notably, the failure to diversify supply chains has illustrated the lack of supply chain resilience within many businesses.

- **Environmental risk**: Climate change is already reducing the economic resilience of many states. In the future, changing weather patterns will also threaten manufacturing production in flood-prone areas and increase food scarcity.

- **Geopolitical risk**: Certain sectors are now dominated by countries where geopolitical tensions are high. China, a strategic competitor, has invested significantly in production and refining capacity of rare-earth materials, which are essential for the fourth industrial revolution. Another country in region of high geopolitical risk, Taiwan, is responsible for the production of a significant proportion of the world’s semiconductors.

- **Technological risk**: Securing digital infrastructure is also a significant challenge for economic resilience. As the issue of 5G technology demonstrates, this is about more than managing cyber risk. The absence of 5G capacity highlights the lack of vendor diversity and the failure to invest in some strategic technologies in the G7.

The chair concluded by drawing attention to historical precedent. This is not the first time that the UK and other G7 members have confronted this kind of challenge. The aftermath of the OPEC crisis in the 1970s illustrates that we have been able to answer these kinds of geopolitical, economic and technological questions before. Some of the same measures that policymakers used in response to that crisis – diversification of supply, geopolitical interventions to protect sources of supply – may well be needed again.
2. Roundtable Discussion: Themes

Following these opening remarks, a roundtable discussion focused on the following themes: supply chain resilience; cyber resilience; strategic competition and sovereign capability; research and development; the role of the G7.

Supply Chain Resilience

Much of the discussion focused on the need for supply chain resilience amid growing geopolitical tension and technological change.

- **The consequences of globalisation**: Several participants suggested that the supply chain issues currently faced by governments and businesses are the consequences of globalisation over the last several decades. Governments did not think about the national security implications of outsourcing, just-in-time supply chains and the drawdown of manufacturing capacity. One participant argued that this was because liberal markets by nature focus more on cost-effectiveness than resilience.

- **Encouraging interdependence**: However, some participants also argued that some aspects of globalisation can increase resilience by encouraging interdependence and heterogeneous supply chains. This is because many businesses and sectors have become too reliant on single points of supply and therefore single points of failure. One participant noted that technological changes are driving us towards interdependence and interconnectivity and that this should be embraced rather than resisted.

- **Public versus private sector priorities**: The challenge of supply chain resilience also highlights that the agendas and objectives of governments and corporations diverge. As a result, their priorities around supply chains are viewed differently. Governments cannot dictate how businesses manage their supply chains but can still have an impact through well-crafted policy.

- **Agility versus resilience**: One participant noted the need to consider agility as well as resilience. Agility is the ability for the supply chain to respond to short-term disturbance. Resilience is about longer-term structural change. Policymakers should primarily concern themselves with dealing with structural changes in supply chains and production, particularly around strategic technologies such as semiconductors.

- **Developing trust and capability**: G7 members need to develop the capability to identify trusted and untrusted suppliers. Then governments must consider what role regulation can play in ensuring resilience in supply chains, as with current UK Telecoms Security Regulations related to 5G. Cyber resilience and supply chain resilience certification schemes could also be developed between like-minded governments to help to build overall resilience.

Cyber Resilience

Participants also discussed the role of cyber resilience in digital infrastructure – a challenge emphasised by the recent SolarWinds supply chain compromise.
• **Securing digital infrastructure**: one participant stressed that the barriers between the digital and analogue economies were eroding, which would impact both individuals and businesses. “Your digital identity will become more important than your physical identity; it will become your priority identity and you won’t be able to participate in society without it”. This is a fundamental change in the impact technology has on society and emphasises the need to secure digital infrastructure.

• **Cyber threats to critical national infrastructure**: Cyber attacks and cyber espionage against healthcare organisations and the vaccine supply chain have also served to re-emphasised the need to ensure cyber resilience for critical national infrastructure. G7 members can do much more to collaborate on securing critical national infrastructure from cyber operations. As one participant noted, ‘Cyber is the only type of risk where we expect a private company to defend itself from a state actor by itself’.

• **The proliferation of cyber capabilities**: The cyber resilience of G7 members’ economies is also threatened by the proliferation of cyber capabilities. Nation-state-level cyber capabilities are becoming easier to access through off-the-shelf tools, commercial spyware providers like NSO Group or so-called ‘hack-for-hire’ groups. Non-state actors might not have the same reasons for restraint as state actors.

• **Creating resilient infrastructure**: Several participants highlighted that a lot of the work the NCSC has done around 5G is transferable to other areas of critical national infrastructure. Need to build in resilience in procurement and incentivising good cyber security standards. G7 members need to influence standards bodies and prevent nations that don’t share our values from taking a disproportionate voice.

**Strategic Competition and Sovereign Capability**

The discussion also highlighted concerns around the extent to which G7 member states have fallen behind China in developing strategic technologies and maintaining economic growth.

• **Competing with China**: Several participants stressed the scale of the geopolitical and economic challenges posed by China – ‘we have got one hell of a challenge on our hands to face the Chinese in a way the Integrated Review is saying’. This challenge has been made more acute by the COVID-19 pandemic, which to many has demonstrated the effectiveness of the Chinese authoritarian political and economic model. The Chinese economy is expected to overtake the US in 2028 and one attendee argued this would have a significant psychological impact on the US and other G7 members.

• **The role of sovereign capabilities**: Participants contrasted China’s approach to investing in sovereign capabilities with the UK’s over the last several decades. One attendee noted that China has made significant investments in strategic technologies like AI, quantum computing and 5G, the production of rare-earth materials, and its manufacturing base. By contrast, ‘the financial system in the G7 has nearly ceased being able to finance the production of anything physical’. As with the challenge of supply chain resilience, the lack of sovereign capability stems in part from the overemphasis on outsourcing physical production to Asia and focusing on software and services – one participant noted that even with increasing strategic competition with China, many G7 policymakers had yet to shift from this mentality.
• **Championing values rather than balkanising**: Attendees discussed several ways in which G7 members can compete with China and develop sovereign capability. One participant suggested that sovereign capability should not mean a drive for ‘sovereign supremacy’, but that policymakers should instead aim to be competitive with China in strategic technologies. One potential way to achieve this is for G7 members to invest in innovation and take on more risk from the private sector. Several participants argued that banning China from supply chains or certain sectors is not a viable option. Rather than ‘balkanising’ the internet and the global economy, policymakers should instead encode the values of western democracies in the technology we build and establish a free and open vision for the internet and the global economy. This vision needs to be championed, as for some middle-ground countries the vision of the internet and technology offered up by more authoritarian states can be more attractive than the western model.

**Research and Development**

Discussions around the implications of strategic competition with China for economic resilience also highlighted the need for increased investment and policy interventions related to R&D.

• **Contrasting approaches to R&D**: Several participants pointed to the contrasting approaches to R&D in China versus the UK. One participant noted that the Chinese government and Chinese businesses have taken a much longer view on investment in R&D – ‘they are thinking in 20-year investment cycles, whereas the West thinks in much shorter cycles’.

• **The shift to private sector R&D**: The discussion also highlighted how in the G7 R&D has shifted from government-funded research to innovation almost wholly funded by the private sector. Similarly, ‘in the West a lot of the brain power is now in the private sector’. However, the private sector has different motivations and objectives to government and is less well-positioned to take long-term risks on innovation. One participant noted that policymakers are yet to understand this change.

**The Role of the G7**

Finally, the participants discussed different measures for improving the economic resilience and competitiveness of G7 member states.

• **Coordinated investment and regulation**: Several participants highlighted the need for more coordinated investment and regulation to remain competitive and secure. One attendee, for example, suggested that the G7 could look to pool resources for semi-conductor fabrication, which is enormously expensive. G7 members have the design capability but not the manufacturing capability to fabricate silicon semiconductors at scale. More broadly, the G7 could look to create a G7 hub of innovation focused on strategic technologies. At the same time, G7 members also need to think about how they can avoid free-riding on each other.

• **Drive international standards to manage risk**: Another lever is for G7 member states to work together to ensure they are influencing international standards – for instance, around telecoms and 5G. As such, they need to get a much deeper understanding of that environment. At the
same time, this process needs to be carried out carefully, as there is a sense that G7 members will be perceived as ‘status quo merchants with our foot on the head of the developing world’.

- **Development financing:** The G7 could also coordinate investment in the developing world. One participant highlighted that many developing countries are currently introducing 4G networks, and that member states could support financing and compete with China in this space.

- **Champion values:** Finally, participants were keen to stress that the G7 should swerve attempts to balkanise the global economy and instead focus on championing their values.

The issues raised in this roundtable go well beyond the confines of supply chain security or cyber risk management. Rather, they are issues of industrial strategy. The G7 should rapidly identify those advanced technology (and other) areas where greater vendor diversity and/or sovereign capability could address these gaps. This will require close co-ordination with allies and partners to share financial investment risk, while aligning the different priorities of governments and industry. One closing remark referred to the importance of regulation among like-minded countries, along with high standards in cyber security and for the green transition.