CR²

COALITION TO REDUCE
CYBER RISK

Alexander Botting

International Director, Coalition to Reduce Cyber Risk

The Global Policy View

- More than 80 national strategies for critical infrastructure in place globally (UNIDIR). Core components:
  - ✓ Define critical infrastructure (who is in scope?)
  - ✗ Security measures requirements (ex-ante requirements)
  - ✗ Process and timeline for incident reporting (ex-post requirements)
  - ? Threat intelligence sharing (addressing information asymmetry)
- So how are we doing in terms of alignment?

The Global Policy View

- This only covers one aspect of cybersecurity. Many governments are also putting forward standards and regulations for:
  - Security of connected devices (IoT security)
  - Network infrastructure security
  - Supply chain security
  - Ransomware
- Ex-ante alignment on principles can help to limit the impact.

Why is this a trade issue?

COALITION TO REDUCE CYBER RISK

1. Threats to cybersecurity undermine confidence in digital trade.

   - Trust is foundational to consumer use of digital ecosystems.

   - Failure to protect consumers and maintain network availability reduces consumer trust.

   - Policies that prevent companies from taking an integrated, risk-based approach undermine the ability of companies to implement cyber best practices globally.

   - Prescriptive policies can (and typically do) prevent companies from taking a risk-based approach

.

Why is this a trade issue?

2. Where cybersecurity laws diverge from international standards and best practices, they reduce market access and competition.
   - Governments can meet cybersecurity objectives by taking a risk-based approach and leveraging international standards.
   - Where governments mandate policies that diverge from this approach, they create inconsistent or conflicting legal requirements on companies.
   - Inconsistent or conflicting legal requirements act as a non-tariff barrier, forcing companies to assess whether requirements are redundant or substantively different and potentially exit a market due to fear of legal risk.
   - The overall effect is to suppress competition and trade, lowering the value proposition for consumers and potentially undermining security operations.

Why is this a trade issue?

3. The use of consensus standards reduces regulatory complexity and facilitates multi-country supply chains.

    - Consistent international use of consensus-based standards enables equal access for companies, no matter their country of origin.

    - The alignment of national policies with these standards reduces complexity for SMEs, enabling them to better understand legal requirements and integrate into global supply chains.

    - Vendors can sell to customers more efficiently when countries adhere to the same set of standards.

Why is this a trade issue?

4. We are seeing an increasing trend of using cybersecurity laws to incorporate protectionist measures that do not enhance security.

   - In many cases these laws are explicitly designed to favor local companies, e.g. requirement to procure cyber insurance from a local company.

   - In other instances, they have the effect of adding direct costs to foreign companies, e.g. through local presence requirements or data localization requirements.

How do cyber laws act as a trade barrier?

1. Unnecessary divergence from consensus standards and best practices creates *de facto* technical barriers to trade.

   - Country by country, Critical Infrastructure operators must manage the cost and complexity of redundant, inconsistent, or conflicting security measures to comply with local cybersecurity laws that share the same objective.

   - Manufacturers may have to certify the same IoT devices in multiple different countries in order to meet the same security objectives.

How do cyber laws act as a trade barrier?

2. Preferential treatment for local providers undermines the principle of equal national treatment.

   - Local presence requirements impose additional costs on foreign companies, since domestic companies *ipso facto* have a domestic presence.

   - Mandatory use of domestically headquartered companies undermines the core WTO principle of equal national treatment by prohibiting foreign companies from competing.

How do cyber laws act as a trade barrier?

3. Local registration and certification requirements establish barriers to cross-border trade in services.

    - By forcing cybersecurity service providers to register or certify country by country, countries introduce cost and complexity that inhibits trade in services.

    - This impact is borne most significantly by:
        - SMEs, which have fewer resources to devote to compliance measures; and
        - Consumers, who pay for redundant certification costs in the price of digital services.

CR²
COALITION TO REDUCE CYBER RISK

How do cyber laws act as a trade barrier?

4. Data localization undermines innovation, competitiveness and security.
    - Data flows support innovation and competitiveness by enabling companies to:
        - Generate security and resilience insights;
        - Improve product performance; and
        - Deploy a global security model that protects data wherever it is stored.
    - Data localization undermines security by:
        - Inhibiting companies' ability to detect fraud and anomalies;
        - Forcing duplication of data and thus the size of the attack surface; and
        - Preventing the use of resilience measures.

How do cyber trade commitments support SMEs?

1. Aligned approaches increase SME participation in the market, fostering competition and encouraging new market entrants.
   - Consistent use of global consensus-based standards facilitates equal access for both suppliers and purchasers.
   - Regulatory divergence forces suppliers to choose between domestic compliance, alignment with international best practices, or costly duplication.
   - Regulatory divergence forces purchasers to exclude capable vendors from their supply chain or diverge from their security standards.

How do cyber trade commitments support SMEs?

2. Consistent use of standards reduces complexity and eliminates compliance costs for SMEs.

    - The incorporation of cyber principles into a trade agreement helps to highlight best practices to non-governmental stakeholders.

    - Avoiding the need to comply with multiple divergent regimes reduces operational complexity for smaller companies, which can be critically important when addressing cyber threats.'

    - Conform once, comply many' eliminates significant compliance costs for businesses.

    - While all companies benefit, this is particularly true for SMEs, which can seldom afford to bear the costs of compliance with multiple regulatory regimes.

.

How do cyber trade commitments support SMEs?

COALITION TO REDUCE CYBER RISK

3. Alignment with international best practices improves security outcomes, reducing the impact of security incidents on SMEs.

   - Purchasers can set expectations among their suppliers regarding the international standards and best practices that are most effective.

   - Requiring alignment with certain best practices drives investment in those areas, such as staff training or penetration testing.

   - Once in the supply chain, vendors are more likely to be privy to threat intelligence and ongoing support from more sophisticated actors.

What language would help to address?

We've seen the emergence of text in at least 2 FTAs: USMCA & US-Japan:

1. *The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:*
   (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and
   (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. *Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.*

This language could be strengthened but is a good starting point.

Cyber language in existing trade agreements

Policy	Forum	Year
Cybersecurity cooperation - Building government capabilities - Cooperate to identify and mitigate intrusions	(CP)TPP	2015-2018
	G20 Finance Ministers Declaration	2018-2019
	RCEP	2020
	Australia-Singapore DEA	2020
Cybersecurity cooperation + Risk management-based approach + Consensus-based standards	USMCA	2018
	Japan-US DTA	2019
	APEC FSDE	2019

CR²

COALITION TO REDUCE
CYBER RISK

Questions