Rules of the Game in the Digital World

Managing the Challenge of Foreign Technologies

Bruce McConnell
Executive Vice President, EWI

EastWest INSTITUTE

Digital Technology is Strategic

Valid Concerns about Security

Solution? Technology Nationalism?

Reality is Different

U.S. Restrictions on Huawei

Chinese Cyber Laws

Supply Chain Assurance

Better Ways to Mitigate Risk

Today's Topics

Digital Technology is Strategic

- National and economic security depend on reliable information and communications technology (ICT) and networks.
- Military preparedness and capability rely on the commercial ICT technologies and networks.
- In a world of increasing conflict, states are becoming more risk-averse about using technology from potential adversaries.

Valid Concerns about Security

- Overall adversarial climate.
- Risky to depend on an adversary for critical technology.

Threats

- Disruption of critical functions.
- Espionage.
- Falling behind in technology competition.
- Trade concerns.

Solution? Technology Nationalism?

- Technology Nationalism, or "TechNationalism," describes direct or indirect policies, measures and actions that favor ICT products and services sold by companies headquartered domestically or in allied states over those headquartered in states seen as competitors or adversaries.

- TechNationalism in the global ICT market is based on state interests which can include national security, cybersecurity, economic competitiveness, innovation, prestige and geopolitics.

TechNationalism Policies and Impacts

	Competition	Innovation	Trade	Deployment	Product Cost	Market Access	Other
Technology Bans and Restrictions	■	■		■	■		■
Technical Security Requirements and Reviews	■	■			■		
Export Controls	■	■	■	■		■	
International Trade Agreements and Tariffs			■			■	
Investment Restrictions		■		■			■
Ownership Limitations							■
Data Localization Requirements				■	■		■
Domestic Technical Standards					■		■

Reality Is Different

- Technology Is Global
- U.S. and China are Leaders (Microsoft, FoxConn)
- 5G Networks Have No Edges
- All Governments Can Influence Technologies

- Result: False Sense of Security, Increased Risk

U.S. Example: Huawei Restrictions

- U.S. Government Purchases of Huawei Tech
- Effective 13 August 2019
- Also applies to ZTE, Hytera, Dahua, Hikvision

- Government Contractors Who "Do Business with Huawei"
- Effective July 2020

- U.S. Technology Sales to Huawei
- Relaxed After G20 Trade Meeting 29 June
- Scope and Timing Uncertain

Example: Chinese Cyber Laws

- Cybersecurity
- Control of Internet Activities (includes Chinese Tech)
- Restrictions on Purchase of Foreign Technologies
- Scope Remains Unclear In Some Cases

- Data Protection and Privacy
- Real-Identity Authentication
- Standards Under Review
- Cross-Border Data Transfers/Localization – Pending

Better Ways to Mitigate Risk: Supply Chain

- Set Security Baselines
- Manage Security in Development
- Inspect, Evaluate and Certify Security
- Manage Security Vulnerabilities
- Operations and Configuration Management
- Transparency and Accountability on Security

Seven Ways to Mitigate Risk

1. Supply Chain Assurance and Transparency
2. Cybersecurity Risk Management by Customers
3. Threat and Risk Information Sharing
4. Smart Sourcing with Diverse Suppliers
5. Strategic Investments in Critical Technologies
6. National Security Exceptions
7. No Tampering

Thank You

bwm@eastwest.ngo

New York | Brussels | Moscow | San Francisco
www.eastwest.ngo | **t:** @EWInstitute | **f:** EastWestInstitute