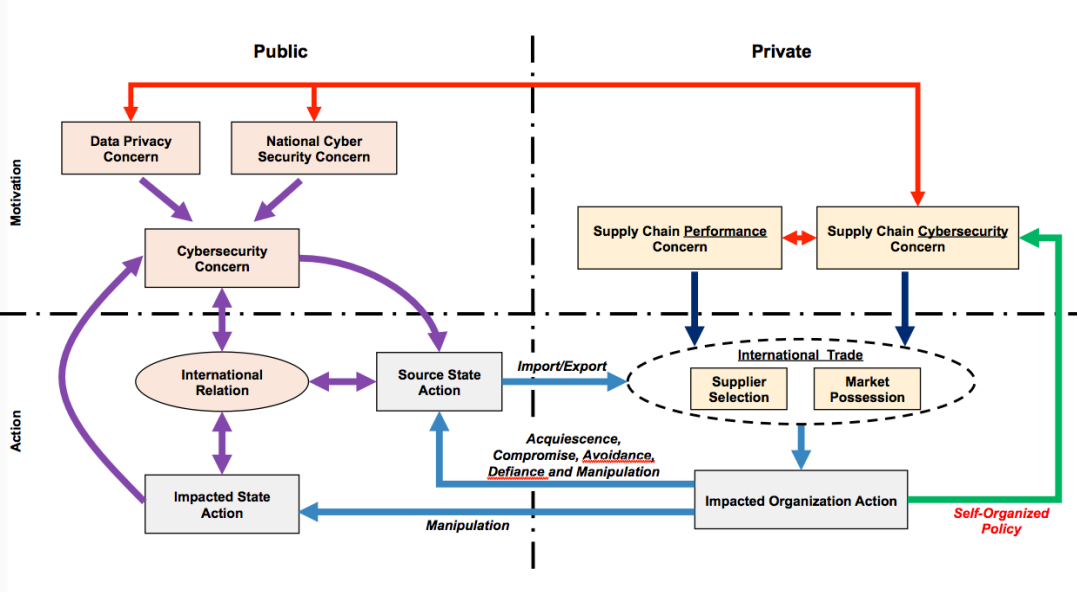Cybersecurity at MIT Sloan brings together thought leaders from industry, academia and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

As the number of products connected to the Internet increases, governments will develop trade policies that impact the flow of goods and services.

Regulating International Trade to Manage Cybersecurity Concerns

Restrictions regarding technology have long existed, but until now, cybersecurity has not been a key issue for trade policy. Almost every modern product is (or can be) Internet connected. Hacking has been reported for items as disparate as cameras, ATMs, medical devices, industrial control systems, cars, and "smart toilets." News reports detail cases where governments are working with private sector companies to incorporate spyware, malware, or other programs in products that are exported around the world. Currently, no specific cybersecurity policies exist to regulate the trade of these items, or monitor their data collection. Incidents have been met with blanket bans of certain items, or items from certain countries. Cybersecurity at MIT Sloan researchers are exploring these incidents to answer important questions about cyber risk and protection in international trade.

IMPACT: This work explores the misuse of internationally sourced IoT products and how their cybersecurity incidents affect trade policy. The research explains how cybersecurity policy will affect trade, and identifies the best options for cybersecurity regulation within the international market.