What Countries and Companies Can Do When Trade and Cybersecurity Overlap

Stuart Madnick, Simon Johnson, and Keman Huang

Working Paper CISL# 2019-03

January 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

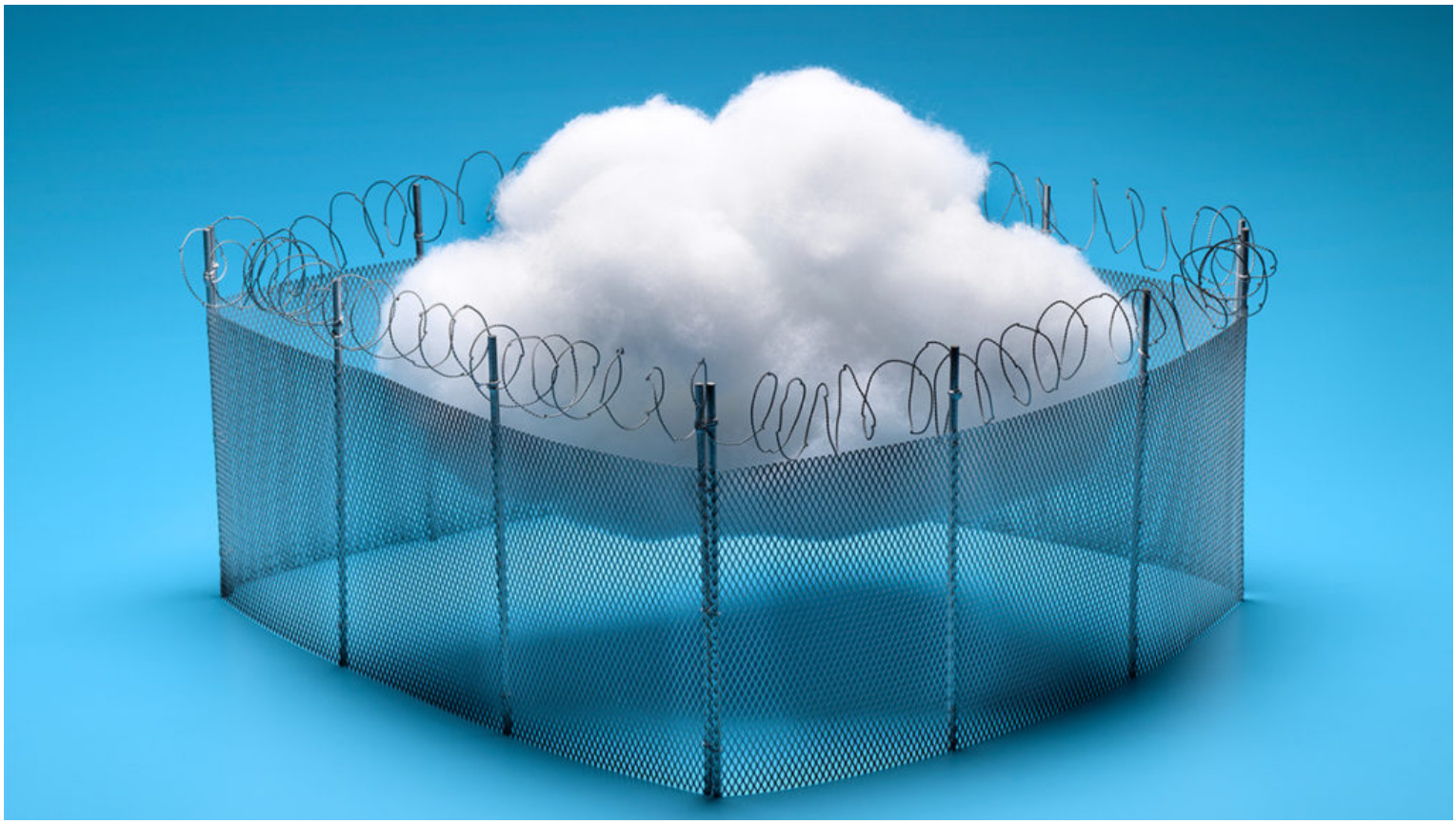
Harvard Business Review

ECONOMICS & SOCIETY

What Countries and Companies Can Do When Trade and Cybersecurity Overlap

by Stuart Madnick, Simon Johnson, and Keman Huang

JANUARY 04, 2019 **UPDATED** JANUARY 04, 2019



JEFFREY COOLIDGE/GETTY IMAGES

Cybersecurity as a key issue for trade policy is a relatively new development. In the last few years there have been a number of news reports about various governments' incorporating spyware, malware, or similar programs into computer-based products that are exported around the world.

The governments typically have worked with private companies in their countries to do it. In the internet-of-things era, almost all products can be connected to the internet, and most of them can also be used for spying and other malicious activities. Furthermore, since data is considered a critical asset, services, from international banking to payment systems to consumer websites, are part of this too.

In late 2016 and 2017, for example, the voice-activated My Friend Cayla doll made headlines for its technology, which could be used to collect information on children or anyone in the room. In 2017 Germany banned the doll, alleging that it contained a surveillance device that violated the country's privacy regulations. Another famous example is the 2010 Stuxnet attack on the Natanz nuclear enrichment facility in Iran. It was accomplished by planting malware, including Stuxnet, into industrial control systems that were shipped to Iran, resulting in the destruction of many centrifuges.

Although trade conflicts involving the U.S. and China, or the U.S. and Russia, have received much attention in the press, cybersecurity-related trade conflict is a truly global phenomenon. As part of our initial research on this topic, we identified 33 cases of a country blocking the import of a product or service due to cybersecurity concerns. In each one, different circumstances and actions led to different outcomes. The cases involved 19 countries all over the world, and in the future it's likely that these kinds of trade conflicts will involve almost all developed countries.

Since it is not feasible to thoroughly examine the software, firmware, and hardware of every single product, what should countries and companies do to prevent cyber intrusions? One seemingly obvious approach is to exclude from import potentially dangerous products from questionable countries. But this approach requires identifying which products are dangerous and which countries are questionable — a formidable task. And such restrictions can quickly become policies, with implications for international trade and the world economy.

Countries and companies need to consider their options. At present, there is no framework for understanding and categorizing the cybersecurity concerns involved in trade. Without a clear understanding, governments may implement policies that result in cyber conflicts, while businesses

will struggle to keep up with how cybersecurity concerns and restrictions are evolving. We have developed a framework to systematically organize these cases, basing it on our in-depth interviews with domain experts.

What Options Do Countries Have?

There are various possible actions that governments can take. Each of the following should be carefully considered:

Do nothing. Governments can accept the potential risk of a cybersecurity situation and choose to ignore it. In 2004, for example, the German Federal Intelligence Service (BND) discovered that the hardware company NetBotz, then based in the U.S., was selling security cameras with a backdoor that sent videos to U.S. military servers. The BND did not disclose that fact until 2015, only after a magazine had discovered and revealed the situation.

Develop import trade barriers. Some nations will take actions to implement trade policies or regulations which will directly restrict the import of international trades, such as Germany's banning of the My Friend Cayla doll.

Restrict government procurement. Governments can prohibit their use and purchase of certain products. For example:

- The U.S. banned government and military systems from using Kaspersky Lab security software and drones made by Chinese company DJI.
- China removed networking equipment from Cisco Systems and security software from McAfee and Citrix Systems from its government procurement lists.

Develop norms of behavior. Countries can agree to not engage in certain types of behavior, such as when the U.S. and China agreed not to conduct the cyber theft of intellectual property for commercial purposes.

Amplify the conflict. On the other hand, some nations can choose an opposite option and escalate the conflict. The U.S. and Russia, for example, have developed a tense relationship, which has been referred to as the "Cold War 2.0."

What Options Do Companies Have?

Although government actions and concerns are often more visible, companies need not play a passive role. They can anticipate these concerns and take actions to reduce or mitigate the consequences. There are various options available:

Recommend action. For example, on August 9, 2017, 10 major cybersecurity companies in the U.S. wrote to Robert Lighthizer, the U.S. trade representative, to urge that he "incorporate cybersecurity trade issues in the upcoming modernization of the North American Free Trade Agreement (NAFTA)."

Acquiesce. As noted earlier, Germany took action against the My Friend Cayla doll, due to concerns about privacy. The company acquiesced and stopped selling it in Germany.

Compromise. Telegram, the end-to-end encrypted messaging app, was threatened with a ban in Russia, so the company agreed to register under the new Russian Data Protection Laws; however, it will not store citizens' information on Russian servers. As another example, Google exited the Chinese market eight years ago to avoid having to censure its search results to meet Chinese government rules. The company has recently decided to reenter, with modest changes to its search engine operation. It is not yet clear that this compromise will be accepted by both parties.

Avoid. Typical examples include Google's withdrawal from China in 2010 and Huawei's withdrawal of its network hardware products from the U.S. in 2014. The latter occurred after the products were removed from U.S. government procurement lists and private telecommunications companies were advised not to purchase Huawei products.

Defy. An organization may challenge or attack cybersecurity regulations. For example, in 2016 LinkedIn challenged the Russian Data Protection Laws, stating that it would not move Russian user data to the country. As a result, Russia blocked LinkedIn in 2017.

Collaborate. Finally, organizations can choose to work with countries to mitigate the negative impact of regulations, or even to be involved in the regulation-making process. An example of this is how Huawei has worked with the UK government.

In 2011, worried about potential spying, the U.S. government rejected a bid from Huawei to build a new national wireless network for first responders. This was followed by further government restrictions on Huawei. Finally, in 2014, Huawei decided to exit the U.S. market.

The UK, on the other hand, does use the company's technology in national infrastructure. In 2010 it opened the Huawei Cyber Security Evaluation Centre to monitor concerns about the technology's use. This was followed in early 2014 by the establishment of an oversight board, which every year releases a report about any risks from Huawei's involvement in UK's critical networks. It should be noted, however, that the oversight board's 2018 report raised serious new concerns about Huawei's technology and the security risks it could pose to UK security.

As the digital economy continues to develop, cybersecurity will play a critical role in international trade. Instead of considering security only a regulation issue, governments need to consider ways to avoid unnecessary confrontations, and organizations should become proactively involved to address concerns and influence policy to improve outcomes for everyone.

Authors' note: The research reported herein was supported in part by the MIT Internet Research Policy Initiative, which is funded by the Hewlett Foundation, and Cybersecurity at MIT Sloan, which is funded by a consortium of organizations.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.

Simon Johnson is the Ronald A. Kurtz (1954) Professor of Entrepreneurship at the MIT Sloan School of Management, where he is also head of the Global Economics and Management group and chair of the Sloan Fellows MBA Program Committee.

Keman Huang is a Research Scientist at the MIT Sloan School of Management, where he works on cybersecurity management and policy, innovation ecosystems, and big data analysis.

This article is about ECONOMICS & SOCIETY

FOLLOWING

Related Topics: SECURITY & PRIVACY

Comments

Leave a Comment

POST

1 COMMENTS

Result Kit 4 hours ago

Dear Authors,
Thanks a lot. Recently in Bangladesh, Bangabandhu Sheikh Mujibur Rahman Digital University, first digital university in the country, academically get introduced Cybersecurity subjects. University received approval from Bangladesh University Grants Commission for conducting educational programs in Digital Learning and Cybersecurity certificate courses under the Institute for Online and Distance Learning. Googling Cybersecurity I reach this article.
Thank you very much. I gain a lot of knowledge.

REPLY

0 0

JOIN THE CONVERSATION