A REPORT OF THE CSIS
HILLS PROGRAM ON GOVERNANCE

National Security and China's Information Security Standards

OF SHOES, BUTTONS, AND ROUTERS

Author
Nathaniel Ahrens

November 2012

50 YEARS | CHARTING OUR FUTURE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A REPORT OF THE CSIS
HILLS PROGRAM ON GOVERNANCE

National Security and China's Information Security Standards

OF SHOES, BUTTONS, AND ROUTERS

Author
Nathaniel Ahrens

November 2012

50 YEARS | *CHARTING* OUR FUTURE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS—50th Anniversary Year

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Since 1962, CSIS has been dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. After 50 years, CSIS has become one of the world's preeminent international policy institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global development and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. John J. Hamre became the Center's president and chief executive officer in 2000. CSIS was founded by David M. Abshire and Admiral Arleigh Burke.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Cover photo: Security system, © iStockphoto.com/enot-poloskun/Andrey Prokhorov.

ISBN 978-0-89206-757-2

Center for Strategic and International Studies
1800 K Street, NW, Washington, DC 20006
Tel: (202) 887-0200
Fax: (202) 775-3199
Web: www.csis.org

CONTENTS

NATIONAL SECURITY AND CHINA'S INFORMATION SECURITY STANDARDS
OF SHOES, BUTTONS, AND ROUTERS

Nathaniel Ahrens

Overview

As part of a concerted effort to promote indigenous innovation, Chinese policymakers have crafted a set of information security standards entitled "Regulations on Classified Protection of Information Security."[1] These protectionist standards, instituted under the guise of national security, are problematic for China, China's trading partners, and the World Trade Organization (WTO). This briefing will analyze the legal aspects governing these regulations and suggest possible courses of action and remedies.

Recently, both the European Union (EU) and Japan have officially reiterated requests through the WTO's Committee on Technical Barriers to Trade (TBT) that China clarify policies relating to its information security (infosec) standards.[2] The United States, both bilaterally and in TBT committee meetings, has also been pushing for clarification since the release of the Chinese government measures in 2007.[3] To date, China has not made these measures one of its 695 TBT notifications, but, with pressure mounting, the country may soon have to submit. Not only could these infosec measures have far-reaching commercial consequences, but, if parties are not careful, they may also result in a long-averted delineation of the national security exceptions in the General Agreement on Tariffs and Trade (GATT) and other related WTO legal documents.

In June 2007, China introduced new regulations governing the information technology industry, the Regulations on Classified Protection of Information Security.[4] According to the four

Note: This discussion was originally prepared for the Johns Hopkins University Paul H. Nitze School for Advanced International Studies and has been since modified. The author wishes to thank Amy Porges, Joshua Meltzer, and Alex Woods for their comments and suggestions.

1. There are now at least 11 interwoven regulations relating to the RCPIS measures. These are listed, along with their relationships in Yanwei Song, Qinde Ma, and Jian Zhang, "Xinxi anquan dengji baohu zhengce he biaozhun tixi zongshu [Classified protection of information security policies and standards system summary]," *Jishu Guangjiao* [Broad angle for technology], June 2010, 60.
2. See WTO documents G/TBT/M53, G/TBT/27, and G/TBT/W/326, 342, and 344 under the Transitional Review Mechanism pursuant to Section 18 of the Protocol on the Accession of the People's Republic of China.
3. Office of the United States Trade Representative, *2011 Report to Congress on China's WTO Compliance*, Executive Office of the President of the United States, December 2011, 55.
4. Ministry of Public Security, State Secrecy Bureau, State Cipher Code Administration and Information Office of the State Council, "Xinxi anquan dengji baohu guanli banfa [Regulation on classified protection of information security]," Doc. 43, June 22, 2007, http://www.atmb.net.cn/web/UploadFile/2010111094513690.pdf. In light of the lack of official translations, for the sake of accuracy all translations are the author's own. The translation of the title is according to the Chinese preference of "Regulation on Classi-

government organizations that jointly issued the regulations, the measures have the following purpose, declared on the first page of the regulation notice:[5]

> In order to accelerate the classified protection of information security, standardize the administration of the classified protection of information security, improve the ability and level of safeguarding information security, maintain national security, social stability and public interests, and safeguard and enhance the informatization process, the Ministry of Public Security, the State Secrecy Bureau, the State Cipher Code Administration, and the Information Office of the State Council formulated the Regulations on Classified Protection of Information Security, which are hereby printed and distributed to you for your earnest implementation.[6]

These broad and far-reaching regulations (often referred to in English as the Multi-Level Protection Scheme, or MLPS)[7]—in theory aimed at protecting China's national security—actually serve to protect a great swath of Chinese industry from international competition. While in some cases the national security claims may be valid, these regulations appear to overstep the standard definition of national security in WTO law. Even though national security clauses in WTO treaty texts have yet to be ruled on by a dispute settlement board, these regulations threaten to change that—a result that would not be in the interests of the United States or China.

Background: Standards and Indigenous Innovation

China's push for the development of indigenous innovation and standards is an important context for evaluating that country's current measures to protect information security.[8] While China's extraordinary economic success has been evident for the past three decades, Chinese industry faces increasing pressure to move from labor-intensive, low-value-added activity into more productive, higher-value-added areas. In fact, China's ability to move up the industrial value chain is an important precondition for the country's continuing rapid economic and social development. An important aspect of moving up the value chain is the further development of indigenous Chinese technological capabilities. Indigenous innovation plays a critical role in industrial upgrading, as

---

fied Protection of Information Security," although a more accurate direct translation would be "Administrative Measures for the Graded Protection of Information Security."

5. The four organizations are the Ministry of Public Security, National Administration for the Protection of State Secrets, State Cryptography Administration, and the Informatization Working Office of the State Council (whose responsibilities have since been subsumed into the Ministry of Industry and Information Technology).

6. "Xinxi anquan dengji baohu guanli banfa [Regulation on classified protection of information security]," 1.

7. The term *MLPS* was coined by the United States Information Technology Office, an industry trade association. This discussion will use the Chinese abbreviation RCPIS. The Chinese representative to the Committee on Technical Barriers to Trade in the WTO stated that RCPIS is the correct name during a meeting on March 24–25, 2011. See WTO document G/TBT/M/53.

8. For a more detailed discussion, see Dieter Ernst, "Indigenous Innovation and Globalization: The Challenge for China's Standardization Strategy," East-West Center and University of California Institute on Global Conflict and Cooperation, June 2011, 19–40; Scott Kennedy, "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars," *Asia Policy* 2 (July 2006): 41–62; and Nathaniel Ahrens, "Innovation and the Visible Hand: China, Indigenous Innovation, and Government Procurement" (Carnegie Papers 114, Carnegie Endowment for International Peace, Washington, D.C., 2010), 6.

there comes a point in economic development in which continued dependence on technology inflows begins to inhibit growth. And it is at that point that indigenous innovation becomes essential for continued growth, productivity increases, and wage increases.[9]

The Chinese government has strongly encouraged indigenous innovation and has explored various policies to support these goals. The "blueprint" for this is China's "Outline for Medium- and Long-Term Plans for Science and Technology Development (2006–2020)."[10] A number of other plans and programs from the Ministry of Science and Technology, like China's 863 Program, also support the development of indigenous innovation.[11]

Part of this strategy focuses on standards. Since accession to the WTO in 2001, China has become acutely aware of the importance of standards and the role of government in stimulating innovation. As Chinese firms attempt to move up the industrial value chain into higher-value-added goods and services, they are often stymied by royalty payments due to foreign companies. For instance, in a now-commoditized technology product like a DVD player, the royalties due to foreign companies are often close to half the end sales cost of the device.[12]

In a report on China's standardization strategy, Dieter Ernst provides a comprehensive analysis of the role of the state in promoting the development of Chinese standards. Ernst lists a number of explicit priorities laid out by the government as part of a unified strategy, including the state's maintaining a key role as a coordinator of integrated standards, using standards to promote indigenous innovation, prioritizing strategic emerging technology sectors, and requiring stringent conformity assessment regulations as a means of controlling access to the market.[13]

While promoting indigenous innovation is generally a laudable goal, Chinese policymakers have too often appeared to interpret indigenous innovation as simply import substitution and local protectionism. Some appear to assume that protection of domestic Chinese companies allows these firms to establish standards and intellectual property of their own. Not only is this approach unsupported by theory, but also it is not borne out by experience. China's efforts to date to develop homegrown standards such as WAPI and TD-SCDMA have been mostly unsuccessful.[14]

Put simply, the current innovation drive has often resulted in the adoption of protectionist measures against foreign standards, products, and services. Viewed in this light, the 2007 information security measures appear to be a thinly disguised attempt to protect a large, critical swath of the technology industry from international competition.

---

9. Dieter Ernst, "Global Production Networks and the Changing Geography of Innovation Systems: Implications for Developing Countries," East-West Center Working Papers no. 9, Economic Series (Honolulu, 2000), 23.

10. State Council of the People's Republic of China, "Guojia zhongchangji kexue he jishu fazhan guihua gangyao [Outline for medium- and long-term plans for science and technology development], 2006–2020," February 9, 2006, http://www.gov.cn/jrzg/2006-02/09/content_183787.htm.

11. A list of these key policies in English can be found on the Ministry of Science and Technology website, http://www.most/gov.cn/eng/programmes1.

12. Indrajit Basu, "China and the Art of (Standards) War," *Asia Times*, April 13, 2006, http://www.atimes.com/atimes/China_Business/HD13Cb05.html.

13. Ernst, "Indigenous Innovation and Globalization," 20–21.

14. See Ernst, "Indigenous Innovation and Globalization," 68–100; and Kennedy, "The Political Economy of Standards Coalitions," 45–61.

This suspicion is further supported by the inclusion of next-generation information technology (IT) products as one of the seven strategic emerging industries listed in China's Twelfth Five-Year Plan. The plan highlights the importance of developing domestic capabilities in indigenous innovation and singles out IT as one of the critical industries. The existence of a national-level goal to promote a specific industry combined with a national security measure that protects much of that industry from foreign products puts considerable pressure on China to clarify the rationale for many of the areas covered by these measures.

Analysis of the Information Security Measures

The Regulations on Classified Protection of Information Security (RCPIS) were issued June 22, 2007.[15] These measures built on the foundation created in 1994 by the Regulations of the People's Republic of China for Security Protection of Computer Information Systems.[16] The RCPIS is, in essence, a response to Article 9 of the 1994 regulations, which stipulate that there should be classified (graded) protection levels and that the criteria for classification, definition of grades, and specific regulations should be determined in the future by the Ministry of Public Security and other related departments.[17]

While graded security systems are not problematic in principle (in fact, they are widely used globally), aspects of China's RCPIS are troubling. Under the Chinese regulations, information systems are to be classified as one of five security grades (I–V). Article 6 of the RCPIS explains that the determination of the grade depends on the system owner's *self-classification*.[18] The owner must base this determination on the system's perceived "degree of importance to national security, economic development, and social life, and the effect on national security, social order, public good, and the level of harm posed to the legal rights of citizens, legal persons, and other organizations in the case that the information system is destroyed, as well as other factors."[19]

The area of primary concern with respect to the WTO is Grade III. Grade III classification occurs when "damage of the information security system will cause serious harm to social order and public interest, or cause harm to national security."[20]

If classified as such, according to Article 21 of the RCPIS, Grade III systems and above[21] must fulfill the following criteria (among others):

---

15. There are now at least 11 interwoven regulations relating to the RCPIS measures. These are listed, along with their relationships, in Song, Ma, and Zhang, "Xinxi anquan dengji baohu zhengce he biaozhun tixi zongshu," 60.

16. State Council of the People's Republic of China, "Regulations of the People's Republic of China for Security Protection of Computer Information Systems," Decree 147, February 18, 1994.

17. Ibid., Article 9.

18. According to an expert, however, the line ministry and the Ministry of Public Security have the ability to overrule the self-classification. The emphasis in the text is the author's.

19. "Xinxi anquan dengji baohu guanli banfa [Regulation on classified protection of information security]," Article 6.

20. Ibid., Article 7.

21. The Chinese text reads "三级以上" which has been interpreted to mean *including* level 3. This is how it has been interpreted in the United States and China so far, according to individuals involved in the discussions. This wording could also be read to mean "above level three." It seems that in most cases it is interpreted in legal situations to mean including said number, although Chinese law is unclear in this regard. For reference see http://lawprofessors.typepad.com/china_law_prof_blog/files/YiShangYiXia.pdf.

- The organization that developed/manufactured the product must be invested by a Chinese citizen or legal person, be state-invested or state-controlled, and have independent legal status within the People's Republic of China.
- The core technology/critical components of the product shall have Chinese indigenous intellectual property rights.[22]

Furthermore, the evaluation of systems classified as Grade III and above (conformity assessment procedures) is to be performed by an agency that fulfills the following criteria (among others):

- Was established in the People's Republic of China (excluding Hong Kong, Macau, and Taiwan).
- Is an enterprise or public institution that is invested by Chinese citizens, Chinese legal persons, or the State (excluding Hong Kong, Macau, and Taiwan).
- All of its staff are Chinese nationals.[23]

Up to this point in the analysis of the RCPIS, there are not necessarily any contentious WTO legal issues, although flags are raised by the domestic-content mandates; legal ramifications hinge on how Grade III classification is determined and then on the scope of product coverage.

The determination of Grade III depends on the interpretations of the five key terms in the Grade III definition (emphasis added): "damage of the information security system will cause *serious harm* to *social order* and *public interest*, or cause *harm* to *national security*."[24] Realizing this, the Chinese government has issued guidelines for interpreting these terms:[25]

- *National security* includes matters that affect:
  - The nation's economic competitiveness and scientific and technological strength
- *Social order* includes matters that affect:
  - The orderly work of state organs relating to social management and public service
  - The order of various types of economic activity
  - The order of various kinds of research or manufacturing
  - The legal constraints and moral standards of the public's normal social order
  - Other matters that affect social order
- *Public interest* includes matters that affect:
  - Social members' use of public infrastructure
  - Social members' obtaining public information resources
  - Social members' receiving public services and related aspects
  - Other matters that affect public interest

22. Ibid., Article 21.
23. Ibid., Article 22. Item 3 is listed as item 4 in the unedited original.
24. Ibid., Article 7. Emphasis is the author's.
25. "Xinxi anquan jishu xinxi xitong anquan dengji baohu diji zhinan [Information security technology—classification guide for classified protection of information system security]," National Standard GB/T 22240-2008, Article 5.3, People's Republic of China. For the sake of brevity and clarity, only the excerpts that are relevant to this discussion are noted. Emphasis is the author's.

The other terms are *harm* and *serious harm*. First, how does one determine harm? According to the same government regulations, harm is evidenced by the following conditions occurring after damage:[26]

- The working performance of the functions is affected
- Results in a decrease in the service capacity
- Causes legal dispute
- Results in financial loss
- Brings about unhealthy social consequences
- Causes loss to other organizations or individuals
- Other effects

After harm has been determined to have occurred, the next question is whether it is "standard harm," "serious harm," or "very serious harm":[27]

- *Standard harm:* working performance is partially affected; service ability is somewhat decreased, but primary functionality is not affected; relatively minor legal problems occur; relatively low financial loss; limited unhealthy social consequences; loss to other organizations or individuals is minor.
- *Serious harm:* working performance is seriously affected; service ability is markedly decreased and seriously affects the primary functionality; relatively serious legal problems occur; relatively high financial losses; relatively large range of unhealthy social consequences; loss to other organizations or individuals is serious.

The wide scope, flexibility, and subjectivity involved with all these five terms (serious harm, social order, public interest, harm, and national security) are staggering.

Moreover, the number of industries affected by the RCPIS is potentially enormous. One official Chinese government document states that the information systems of the following industries and government organizations are to be covered:[28]

- Public transmission networks of telecommunications, radio, and television; transmission networks of broadcast television and other foundation information networks; and operational public Internet information service units, Internet connectivity service units, data centers, and related important information systems
- The important websites and office information systems of Party and government organizations at the city level or above
- Railroad, banking, customs, tax, civil aviation, power, securities, insurance, foreign affairs, science development and reform, defense technology, public safety [police], human resources/

26. Ibid., Article 5.4.1.

27. In the determination of the harm level for social order, public interest, or national security, the base for judgment is the effect on the entire industry or country. For level 3, only standard and serious harm are relevant.

28. Ministry of Public Security, "Guanyu kaizhan quanguo zhongyao xinxi xitong anquan dengji baohu dingji gongzuo de tongzhi [Notice regarding the launch of classified protection of national important information systems classification work]," 861, 2007.

> labor and social welfare, finance, audit, commerce, water facilities, land and resources, energy, transportation, culture, education, statistics, industrial and commercial administration, post and related industries, sectors of production, dispatch, management, office administration, and other important information networks

One of the agencies licensed to perform conformity assessment displays a very similar, perhaps more extensive, list on its website.[29] Due to the unique structure of the Chinese government and extensive reach of the state and Party in these areas, it is fair to conclude that coverage is not limited to just the administrative offices of these government bureaus. As an example, a document published by China Unicom engineers in the journal *Broad Angle for Technology* explains the RCPIS as it relates to the telecommunications industry. In that journal, they suggest that the following types of technology could possibly be affected: operating systems, databases, networks, public key infrastructure, gateways, servers, intrusion detection, firewalls, routers, switches, and others.[30]

In a recent communication to China through the Committee on Technical Barriers to Trade, the Japanese delegation stated that, if these measures are implemented, "the commercial impact might be tremendous."[31] The EU followed up with a similar complaint several weeks later, stating that as the RCPIS has come into existence it is

> gradually taking over sectors of the economy not regarded as critical to national security anywhere else in the world—from public utilities companies to banks, mobile phone companies or civil aviation. As a result, reference to MLPS compliance in calls for tenders issued by state-owned enterprise [sic] in the affected sectors are increasingly common, and the number of information systems classified in levels three and above...has increased exponentially—thus excluding foreign and foreign-invested IT providers from several economically very significant segments of the Chinese market.[32]

The *2011 Report to Congress on China's WTO Compliance* states that "to date, hundreds of requests for proposals (RFPs) incorporating MLPS requirements have come from government agencies, the financial sector, telecommunications companies, the power grid, educational institutions, and hospitals in China."[33]

Given the wide scope of coverage, the immense latitude in classification determination, and the number of assessment procedures performed only by Chinese nationals (which, depending on product type and classification level, also involve revealing source code and undergoing testing and certification processes), it is not surprising that these regulations are being raised within the context of the WTO.

---

29. China Information Technology Security Evaluation Center, http://www.itsec.gov.cn/bzfg/xgfl1/1602.htm.

30. Song, Ma, and Zhang, "Xinxi anquan dengji baohu zhengce he biaozhun tixi zongshu," 61.

31. "Questions and Comments from Japan to China," under the Transitional Review Mechanism Pursuant to Section 18 of the Protocol on the Accession of the People's Republic of China, October 21, 2011, WTO document G/TBT/W/342, Section III:4.

32. "Communication from the European Union," under the Transitional Review Mechanism Pursuant to Section 18 of the Protocol on the Accession of the People's Republic of China, November 9, 2011, WTO document G/TBT/W/344, Section 7.

33. Office of the U.S. Trade Representative, *2011 Report to Congress on China's WTO Compliance* (Washington, D.C.: USTR), 55.

The WTO Legal Environment

There are a number of troubling issues with the RCPIS, but the most obvious of these is the domestic-content mandate. This mandate is a clear violation of the national treatment principles laid out in the GATT. The RCPIS may also infringe on the General Agreement on Trade in Services, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the TBT, both of which have national treatment clauses similar to those in the GATT.

Article III (1), of the GATT, "National Treatment on Internal Taxation and Regulation," requires that treatment accorded foreign goods be not less favorable than that accorded domestic goods:

> The contracting parties recognize that internal taxes and other internal charges, and laws, regulations and requirements affecting the internal sale, offering for sale, purchase, transportation, distribution or use of products, and internal quantitative regulations requiring the mixture, processing or use of products in specified amounts or proportions, should not be applied to imported or domestic products so as to afford protection to domestic production.

Furthermore, GATT Article III (4) prescribes the following further requirements:

> The products of the territory of any contracting party imported into the territory of any other contracting party shall be accorded treatment no less favourable than that accorded to like products of national origin in respect of all laws, regulations and requirements affecting their internal sale, offering for sale, purchase, transportation, distribution or use.

Article III has often been invoked in dealings with de facto discrimination, but, in this case, RCPIS is a clear de jure infringement of the national treatment principles of the GATT.

Article III contains a relevant exception that would allow for some purchases to be made on a discriminatory basis. Article III (8) (a), states that the above does not apply to "laws, regulations or requirements governing the procurement by governmental agencies of products purchased for governmental purposes and not with a view to commercial resale or with a view to use in the production of goods for commercial sale." Therefore, for government purchases, under which some of the aforementioned product categories fall, these measures may be defensible.[34] This would not be the case with most state-owned enterprises, however, as the terms of China's accession state that China must "refrain from taking any measure to influence or direct state trading enterprises as to the quantity, value, or country of origin of goods purchased or sold."[35]

Other parts of WTO law are possibly relevant here. GATS Article XVII has similar language, but it covers only those sectors in the schedule:

> In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers.

34. Especially as China has not yet acceded to the Government Procurement Agreement.

35. WTO, *Protocol on the Accession of the People's Republic of China*, WT/L/432 (November 10, 2001), Section 6.1.

In the TRIPS, the national treatment principles are repeated in Article 3:

> Each Member shall accord to the nationals of other Members treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property.

Finally, in the TBT, which covers the use of standards, regulations, and certification, national treatment principles are also codified:

> 2.1. Members shall ensure that in respect of technical regulations, products imported from the territory of any Member shall be accorded treatment no less favourable than that accorded to like products of national origin and to like products originating in any other country.
>
> 2.2. Members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. For this purpose, technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks non-fulfilment would create. Such legitimate objectives are, inter alia: national security requirements; the prevention of deceptive practices; protection of human health or safety, animal or plant life or health, or the environment. In assessing such risks, relevant elements of consideration are, inter alia: available scientific and technical information, related processing technology or intended end-uses of products.
>
> 2.3. Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems.

The RCPIS measures may infringe on all the above depending on the item in question, but the majority of the products are goods, not services, and are tangible ones at that, and thus more likely covered by the GATT than GATS or TRIPS. The possible defenses that could be invoked by China (see below) also lead one to conclude that this is a GATT issue.

And while this issue is being raised within the TBT, it is not clear that security regulations would be governed under that agreement, as it is not the regulation, standard, or conformity assessment that is initially in question, but the straightforward de jure product discrimination.[36] While the RCPIS measures deal with how technical products are to be graded, the first issue is whether China can exclude foreign products from a market based on their end use. After this, additional questions may surround the regulations themselves and the conformity assessment procedures. Rather than establishing a technical standard, the RCPIS seems more an attempt to designate a portion of the domestic market as off limits to foreign products. It is this author's belief that requiring a certain class of product to be of domestic origin is not in itself a technical stan-

36. If the law were loosened then, there may be some technical-barriers-to-trade issues, as there are more widely used standards available internationally, such as the Common Criteria. Conformity assessment procedures might also be problematic (TBT articles 5–8). In some cases, the assessment will require the sharing of source code and encryption standards.

dard.[37] That said, there are compelling reasons why this should still be raised within the context of the TBT, which will be discussed in the conclusion of this report.

Possible Defenses Invoked by China

Chinese regulators, no doubt, realize that this kind of trade-limiting product discrimination is not permissible. It is reasonable to conclude then that China plans to avail itself of an exception. As the primary references in this law are to national security and social order—and, to a lesser extent, public morals—China is likely to try to claim a national security exception, probably under GATT Article XXI.

Invoking a national security exception would be risky, and China would have to argue very carefully to prevail. At a time when Doha is in serious doubt, use of the national security defense could be crippling to the WTO, as it could result in the removal of a huge portion of the global market for IT goods and services from the WTO's practical jurisdiction.

The national security exceptions in the GATT and other WTO treaty documents have rarely been invoked, and their scope has traditionally been viewed as self-defined by the invoking member. Yet despite the wide latitude in determining definition and coverage, that latitude should not be deemed the same as without limits at all.

A number of WTO legal provisions allow invocation of national security exceptions. GATT Article XXI, and specifically XXI (b), is generally seen as the core of the national security exception, but GATS Article XIVbis and TRIPS Article 73 are also relevant.[38]

The danger has always been that since the national security exceptions are so general they could be invoked by any country for any reason, making any trade dispute dead on arrival in Geneva. So far, countries have refrained from taking more than a couple of steps down this slippery slope.[39] One of the most memorable cases occurred in 1975, when Sweden invoked a national security exception to place import quotas on various types of footwear:

> The continued decrease in domestic production has become a critical threat to the emergency planning of Sweden's economic defence as an integral part of the country's security policy. This policy necessitates the maintenance of a minimum domestic production capacity in vital industries. Such a capacity is indispensable in order to secure the provision of essential products necessary to meet basic needs in case of war or other emergency in international relations.[40]

Sweden revoked the measure in July 1977 after complaints from other members, who convinced Sweden that this was not a national security concern. This case aptly demonstrates how, if abused, the national security clauses could be used for almost any product. And since the use is at the discretion of the invoking member, it could then be an effective answer for each and every

37. A helpful discussion on TBT coverage can be found in Peter Van den Bossche et al., "WTO Rules on Technical Barriers to Trade," Maastricht Faculty of Law Working Paper 2005/6, University of Maastricht, Maastricht, The Netherlands. See also annex 1 of the TBT.

38. TBT Article 5.4 is also relevant for conformity assessment procedures.

39. Related cases are discussed collectively in WTO, *Analytical Index of the GATT* (Geneva: WTO, 1994), 599–611.

40. GATT, "Sweden—Import Restrictions on Certain Footwear," November 17, 1975, L/4250: Section 4, 3.

trade dispute. Premier Nikita Khrushchev once mocked U.S. export controls by saying that there should be an embargo on buttons, since they can be used to hold a soldier's trousers up.[41]

National security exceptions have yet to play a significant role in GATT decisions. Other than the Swedish footwear issue, only six disputes have involved national security and only one of those occurred in the WTO era.

In 1949, the United States banned the exports of certain goods it considered "war materials" to Czechoslovakia. The United States invoked Article XXI, among others, but the decision was made in favor of the United States without resorting to that particular article by focusing on the legality of export licenses.[42]

On November 30, 1982, a decision was adopted that clarified the fact that despite the European Economic Community's, Australia's, and Canada's imposition of trade restrictions on Argentina, Argentina still retained full rights under the General Agreement. The decision further stated that such trade measures should be explained to the other party to the fullest extent possible. It also included text that specifically raised the prospect of a future formal interpretation of GATT Article XXI.[43]

Perhaps the most interesting dispute to involve national security centered on the 1985 U.S. embargo on trade with Nicaragua.[44] The report states the following as background:

> The representative of the United States objected to the establishment of a panel. His Government's actions against Nicaragua were covered by Article XXI (b) (iii). This provision left it to each contracting party to judge what actions it considered necessary for the protection of its essential security interests. A panel could therefore not address the validity of, nor the motivation for, the United States' invocation of Article XXI (b) (iii).[45]

While this seems as though it would have led to an Article XXI decision, due to the very narrow terms of reference accepted for the case, the panel was not able to make a decision on the Article XXI claim.[46] At the end of the decision, however, the panel remarked on the dangers of claiming an Article XXI exception in a case like this:

> If it were accepted that the interpretation of Article XXI was reserved entirely to the contracting party invoking it, how could the CONTRACTING PARTIES ensure that this general exception to all obligations under the General Agreement is not invoked excessively or for purposes other than those set out in this provision?[47]

41. John Jackson, "Helms-Burton, the U.S., and the WTO," *ASIL Insights* (March 1997).

42. GATT, "Summary Record of the Twenty-Second Meeting," June 8, 1949, CP.3/SR22, http://www.worldtradelaw.net/reports/gattpanels/usexportrestrictions.pdf .

43. GATT, "Decision Concerning Article XXI of the General Agreement," December 2, 1982, L/5426.

44. GATT, "United States—Trade Measures Affecting Nicaragua: Report by the Panel," October 13, 1986, L/6053.

45. Ibid., Section 1.2.

46. Ibid. The reasons for this are complex but can be explored in a scan of the original document at http://wto.org/gatt_docs/English/SULPDF/91240197.pdf. In the end, the report was not adopted, due to Nicaraguan objections.

47. Ibid., Section 5.17.

In addition, a dispute occurred in 1991 in which the European Community invoked Article XXI to impose trade sanctions on Yugoslavia. Yugoslavia argued that the measures were not in conformity with the meaning of Article XXI (b) and (c), opening the door to an interpretation. The proceedings were suspended in 1993, however, when it was determined that when the Socialist Federal Republic of Yugoslavia transformed into the Federal Republic of Yugoslavia composed of Serbia and Montenegro, the original complainant no longer existed and therefore the complaint was invalid.[48] Previously, Ghana had also imposed a boycott on Portuguese goods, justified by invoking Article XXI, but this did not reach the official dispute stage.[49]

The only WTO-era dispute in which Article XXI has been specifically invoked and contested occurred in 1997 and was "potentially one of the most explosive cases to have reached the dispute settlement stage."[50] In this instance, the EU challenged portions of the 1996 Helms-Burton Act, a U.S. embargo on Cuba that also affected third-party countries and their dealings with Cuba.[51] The United States again invoked Article XXI and stated that it did not need to appear before the panel since with a national security exception "a dispute settlement panel was not competent to examine the justification or the motivation of the United States."[52] This assertion brought the issue to a head. If the United States were to win on these grounds, it would set an alarming precedent that could undermine the still nascent WTO; if the United States were to lose, then the U.S. Congress might withdraw support for an international organization that it was already uncomfortable with, again undermining the WTO's legitimacy.[53] Faced with these equally unappealing possibilities, the EU and the United States signed a memorandum of understanding in which they found a way forward without having to complete the WTO dispute resolution process. The proceedings were suspended, and thus the issues regarding application of Article XXI are still open.

Alexandroff and Sharma posit that now "it may only be a matter of time before a substantive ruling on the parameters of Article XXI will be sought....if WTO governments take the opportunity to invoke sanctions where terrorism and national security threats are not readily apparent, but the protection of domestic interest are, or where foreign policy concerns that do not appear to have direct national security implications are dominant...difficult questions could be presented to the WTO."[54]

Thus, while common perception is that the national security exception is rarely invoked and is not a major concern, clearly the issue has been simmering for a while now, saved from boiling over only by a number of opportune releases of steam.

48. *Analytical Index of the GATT*, 604–05.

49. UNCTAD-ICTSD, *Resource Book on TRIPS and Development* (New York: Cambridge University Press, 2005), 807.

50. Alan Alexandroff and Rajeev Sharma, "The National Security Provision—GATT Article XXI," in *The World Trade Organization: Legal, Economic and Political Analysis*, ed. Patrick Macrory et al. (New York: Springer, 2004), 1: 1577.

51. *Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996*, Pub.L. 104-114, 110 Stat. 785, 22 U.S.C. §§ 6021–6091.

52. Alexandroff and Sharma, "The National Security Provision."

53. Ibid., 1578.

54. Ibid., 1578–79.

Is China Justified in Invoking an Article XXI National Security Exception?

If brought into the dispute resolution process, could China win based on an Article XXI exception, and, if so, what are the risks? For practical purposes, Article XXI has been assumed to be a sort of "gentlemen's agreement." This assumption may encourage WTO parties to believe that they have wide latitude in how it is used.[55] A closer examination of Article XXI reveals that it is not as flexible and lacking in ambit as many scholars and trade lawyers have assumed. In fact, it is highly qualified. Traditional emphasis has been placed on certain words and phrases: "*Nothing* in this agreement shall be construed...to prevent any contracting party from taking *any action* which *it considers* necessary for the protection of its essential security interests."[56] This reading focuses on the interpretation that there is no defense against any trade-limiting action that a member country takes if it does so in the name of national security. But this is an overly simplified reading of the treaty text. In fact, that phrase is qualified by the subtext that follows:

(i) relating to fissionable materials or the materials from which they are derived

(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment

(iii) taken in time of war or other emergency in international relations[57]

A closer reading reveals that the operative words are actually "essential security interests" and the three qualifying conditions to which those essential security interests are connected. The first two qualifiers relating to nuclear technology and arms trafficking are fairly narrow. The third, "time of war or other emergency in international relations," is more broad and flexible. The American "war on terror," while probably not a war, could certainly be construed as an emergency in international relations. While there does not seem to be a need to connect the trade-limiting action to the war or emergency in question, it is likely that the member countries and dispute panels would put heavy pressure on a member who chose to, for instance, place an embargo on Chinese steel because of being engaged in a war in Afghanistan.[58]

Thus, not only is there a qualification on the type of situation in which this national security exception can be invoked, but there is also the fundamental phrase "essential security interests." First of all, is it actually a security interest, and, second, is it an essential one? Finally, does the action actually protect those security interests? One could envision a scenario in which domestic steel was required in the fences surrounding a nuclear site, by invoking Article XXI (b) (i). But is the domestic steel really protecting essential security interests?

China could certainly make a case that is more convincing than shoes and buttons, and in a world where a computer worm can target and take down industrial equipment these concerns are

55. This has parallels to how China may have been viewing possible uses of Article XX exceptions, which in the recent Appellate Body ruling on the China–raw materials case turned out to be a faulty assumption.

56. GATT 1947, Article XXI. Emphasis is the author's.

57. GATT 1947, Article XXI(b)(i–iii).

58. Unless of course, hypothetically, the steel industry in question was found to be materially supporting the enemy.

not unfounded.[59] But is this the least-trade-restrictive method available? And do these concerns warrant such broad product coverage? Does a domestic-content mandate fundamentally change the security protection of the information systems in question?

As discussed earlier, China has explicit goals and a suite of supporting policies aimed at promoting indigenous innovation and replacing products and standards from foreign countries. These are sometimes de jure and sometimes de facto, but interpretation by domestic audiences is rarely unclear. With regard to the RCPIS, not only are the regulations de jure, but also Chinese media have made clear that the goal of such policies goes beyond merely national security concerns. One article noted a CITIC Securities report that stated the following:

> The special nature of the information security industry advances the import substitution process. As information security is connected to national security it is not subject to WTO regulations; national mandates will be the primary manner in which to promote import substitution. The release last year of the classified protection notice requires Grade III and above information systems to use domestic equipment, signaling that the curtain on the substitution of foreign products in China's information security product industry has been opened. In the future, as the level of China's indigenous product technology gradually approaches that of mainstream international products, the process of import substitution of information security products is expected to proceed rapidly.[60]

In related GATT jurisprudence, national security has had a much more narrow usage than that proposed above. The Helms-Burton Act is a much more typical usage of the national security meaning.[61] A letter from a U.S. senator stated that "the security exemption has nearly always been used in the context of a trade sanction with the aim of accomplishing a specific political objective or bringing pressure to bear on a rival nation."[62] This is not to say that there are not other valid uses for the national security exceptions, but it emphasizes that until now the ambit has been quite limited.

On the final subtext clause, Article XXI (b) (iii), are we in a time of war or emergency in international relations? It is highly unlikely that there is a good case for this claim, war on terror included.

In conclusion, the RCPIS has many problems. Initially, the coverage goes far beyond the reasonable limits of "essential security interests."[63] While one could creatively construct a scenario for how a malicious piece of code inserted into the web server that hosted the Beijing Municipal Ministry of Culture website could wreak havoc on social order, it is not likely to fall on sympathetic ears in a WTO dispute settlement proceeding. It is hard to argue that the "nation's economic

59. William Broad and David Sanger, "Worm Was Perfect for Sabotaging Centrifuges," *New York Times*, November 18, 2010, A1.

60. "Jisuanji xinxi anquan zhuanti yanjiu baogao [Computer information security special research report]," CITIC Securities, July 12, 2011, http://guba.eastmoney.com/look,300188,4501711063.html. Translation is the author's own.

61. For a more detailed discussion of how the United States defines its essential security interests within the context of Article XXI, see Ryan Goodman, "Norms and National Security: The WTO as a Catalyst for Inquiry," *Chicago Journal of Law* 2, no. 1 (Spring 2001): 101–19.

62. "Busting Up the Cartel: The WTO Case against OPEC," note from the Office of U.S. Senator Frank Lautenberg, http://lautenberg.senate.gov/documents/foreign/OPEC%20Memo.pdf.

63. GATT Article XXI.

competitiveness and scientific and technological strength" are national security concerns. And defining *social order* in a way that includes matters that affect "various types of economic activity" and "research and manufacturing" seems an even greater stretch. Public interest matters are also too broadly defined.[64] This is then put in the hands of each system owner, who is motivated by other regulations to encourage adoption of indigenous innovation products. With regulations this broad, vague, and subjective, not only is transparency lost, but also local abuse is highly likely. According to the RCPIS as it is currently defined, the digital equivalent of buttons and shoes seems very much within the realm of the possible.

Recommendations

To use this opportunity to set an Article XXI precedent or do anything to harm the legitimacy and efficacy of the WTO is surely not a result that would benefit China. Nor would Chinese technology companies with strong international presences, like Huawei, ZTE, or Lenovo, be likely to encourage these measures, despite the fact that they appear to be the prime beneficiaries of them. It is not only China that is trying to move up the industrial value chain into next-generation IT products, but the rest of the world is, too. As Chinese companies expand globally, they are increasingly more understanding of the benefits of an open-trade regime. Measures such as RCPIS could further encourage tit-for-tat protectionism, especially during this period of global economic challenges.

Of course, there are real concerns with regard to information security, and some legitimate uses of the national security exception in this area are possible. The problem with China's RCPIS as they are currently set out is that they are too broad, are open to abuse, and are contrary to international norms. Other ways of dealing with valid security concerns are available that would not act as a thinly veiled trade barrier.

Classified or graded information security schemes are not new, nor are they particularly controversial when applied appropriately to national security systems. The United States first developed a graded security system in 1983: the Trusted Computer System Evaluation Criteria (TCSEC or Orange Book). In 1990, Germany, France, the United Kingdom, and the Netherlands established the Information Technology Security Evaluation System. Canada established its own standard in 1993, the Canadian Trusted Computer Product Evaluation Criteria, drawing on aspects of these existing standards. Since then, the six governments have collaborated to define a common standard to facilitate trade among the parties. This effort resulted in the Common Criteria for Information Technology Security Evaluation, known colloquially as the Common Criteria.[65] Industry organizations such as the Trusted Computing Group also work to define security standards for use across multiple markets. Its trusted platform modules establish security standards that enable manufacturers of certain IT component parts to embed security features in their products, thus enabling lower trade costs.

64. "Xinxi anquan jishu xinxi xitong anquan dengji baohu diji zhinan [Information security technology—classification guide for classified protection of information system security]," Article 5.3.

65. The Common Criteria can be found at http://www.commoncriteriaportal.org/cc/. An excellent discussion of related issues can be found in Dieter Ernst and Sheri Martin, "The Common Criteria for Information Technology Security Evaluation: Implications for China's Policy on Information Security Standards," East-West Center Working Papers no. 108 (Honolulu, 2010).

While China has no reason to automatically adopt the Common Criteria or accept trusted platform modules, surely it is worth engaging with related stakeholders to understand some of the issues that others have encountered in balancing the need to protect information security while keeping trade open. How do other countries deal with delineating what is a national security concern and what is not? What should be dealt with at a national level, and what should be left to private industry? These issues have global dimensions. The nexus of information security and national security raises concerns that every country needs to address. Recent events in the United States relating to Chinese telecommunication providers Huawei and ZTE demonstrate the need to better delineate national security threats in a nondiscriminatory manner.[66]

China should steer clear of using the WTO's national security exceptions to protect the IT industry. China could take some immediate steps to reduce RCPIS Grade III coverage to just those entities that can legitimately be considered essential security concerns (or remove the domestic-content mandate from Grade III), make policies more transparent, and ensure that assessment procedures are in line with international standards.

To the point about the RCPIS being raised within the Committee on Technical Barriers to Trade, despite questionable jurisdiction this is a sensible approach. The TBT offers a venue in which relatively quiet, diplomatic negotiations can ensue, providing a less drastic alternative to bringing a national security exception into the formal dispute settlement process.[67] Furthermore, the TBT does not contain a national security exception, thus allowing the parties to focus on the merits of the standard itself. The United States, EU, and Japan would be wise to keep discussions contained to the TBT too, as they can thereby avoid an escalation of an Article XXI issue.

Most important, if China wants to retain the benefits of the national security exceptions within the context of the WTO, it is imperative that it not force delineation of these exceptions. National security exceptions in the WTO have effectively operated on the principle of subsidiarity, delegating decisionmaking authority to the WTO member countries. At present, there is a substantial margin of appreciation given to these matters that most countries would be reluctant to see narrowed.[68] If China is open to reasonable discussions with other countries on how they are dealing with similar matters, the national security exception should be able to be preserved and information security achieved in the least-trade-restrictive manner possible.

66. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Report by Chairman Mike Rogers and Dutch Ruppersberger of the Permanent Select Committee on Intelligence, U.S. House of Representatives, 112th Congress, October 8, 2012.

67. John Spanogle Jr., "Can Helms-Burton Be Challenged under WTO?" *Stetson Law Review* 27 (1998): 1335.

68. *Margin of appreciation* is a term that has formally been incorporated into the jurisprudence of the European Court of Human Rights. It may be a more appropriate term than *subsidiarity* for understanding the nature of the national security exceptions in the WTO.

ABOUT THE AUTHOR

Nathaniel Ahrens is deputy director and fellow with the Hills Program on Governance at CSIS, where he is in charge of development and is also active in research. He was formerly an adjunct fellow with the CSIS Freeman Chair in China Studies, where he focused on issues relating to China's trade, industrial policy, and innovation. Ahrens is also president of the American Mandarin Society. In 2010, he was a visiting scholar at the Carnegie Endowment for International Peace, where his research focused on climate, energy, and sustainable development issues in China, as well as Chinese national innovation policy and government procurement. Ahrens also runs Golden Road Ventures Ltd., a business development and strategic advisory firm that provides expertise and support for projects in China. Previously, he worked for 10 years in China. He was senior product manager and director of international sales for Intrinsic Technology, a Shanghai-based telecommunications software provider. He also founded Shanghai Pack Ltd., a luxury-brand packaging company based in Shanghai and Paris. Ahrens is a member of the National Committee on U.S.-China Relations, the Institute of Current World Affairs, and the Asia Society, and he serves as an honorary ambassador for the State of Maine. He holds an A.B. from Vassar College and studied at Beijing Language and Culture University. Ahrens speaks English, French, and Mandarin Chinese.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1800 K Street, NW | Washington, DC 20006
Tel: (202) 887-0200 | Fax: (202) 775-3199
E-mail: books@csis.org | Web: www.csis.org

ISBN 978-0-89206-757-2
90000
9 780892 067572