Inside U.S. Trade - 05/17/2013

U.S. Business Associations Urge USTR To Tackle Cyber Issues In TTIP

Posted: May. 16, 2013

U.S. high technology and business associations are urging the Obama administration to include issues related to cybersecurity in the upcoming Transatlantic Trade and Investment Partnership (TTIP) negotiations with the European Union, according to formal comments submitted to the Office of the U.S. Trade Representative last week.

However, Washington-based observers agreed that the extent to which the two sides will really look to tackle these issues in the context of TTIP remains unclear.

According to Bruce Levinson, senior vice president for regulatory intervention at the Center for Regulatory Effectiveness, there is interest on both sides in dealing with "cyber" issues in the upcoming trade talks. But he conceded that it is not always clear what is meant by "cyber" issues, and the variety of "cyber-related" issues raised in public comments on TTIP that were submitted to USTR served to underscore his point.

Possible ideas include closer coordination on responses to cyber attacks; increased information sharing, including in the wake of attacks; new language outlining what constitutes "good behavior" in cyberspace; closer coordination on future cyber-related regulations; joint development of "best practices" for guarding against cyber attacks; efforts to ensure third countries do not use cybersecurity as an excuse to block trade; and better protection of trade secrets.

But several observers noted that one obstacle to an ambitious outcome is that the U.S. and EU frameworks for dealing with cybersecurity are in flux. In particular, both the Obama administration and the European Commission are in the process of working with their respective industries in order to come up with voluntary frameworks that would reduce risks to critical infrastructure by establishing "best practices" for company-level cyber defenses.

With all of these changes going on, it may be difficult for the U.S. and EU to fundamentally change the way in which they interact on cybersecurity issues in the context of a trade agreement, some observers speculated. On the other hand, others argued that these ongoing efforts to improve cybersecurity on both sides of the Atlantic only highlight the opportunity that TTIP presents to help ensure that they do not adopt divergent approaches.

For the Obama administration, one of the fundamental cyber issues relates to the fact that entities in China, at times with the support of the Chinese government, are engaged in economic espionage against U.S. companies, meaning that these entities are stealing the trade secrets of companies, including through cyberspace, and then using those secrets to compete more effectively against their Western counterparts.

David Fidler, an expert at Indiana University's Maurer School of Law, argued in an interview with *Inside U.S. Trade* that U.S. and EU negotiators should agree to not engage in or support economic espionage. This would help to establish an international "norm" on economic espionage -- none exists currently -- and would "ratchet up" the pressure on China to change its aggressive behavior in cyberspace, he argued.

One potential hurdle, however, is the fact that some EU member states, most notably France, have historically engaged in economic espionage themselves. This is different from the U.S. government, which engages in state-to-state espionage but does not conduct or support espionage activities against foreign companies. Still, Fidler said the EU might be willing to reach an agreement on a global "norm" due to the benefits it could bring vis-a-vis third parties like China.

One EU official agreed that it might be useful for the two sides to use the trade agreement to further delineate what "good behavior" in cyberspace means, but said it is too early to know what the two parties will attempt in TTIP.

Another possible option would be to use TTIP to increase information sharing in the aftermath of cyber attacks, or even to coordinate joint responses, both of which are mentioned in comments on TTIP submitted last week by the group TechAmerica. "In order to defend against the global threat, the U.S. and EU need to collaborate to build capacity, share analysis and information, and respond to attacks," it wrote in a section devoted solely to cybersecurity.

However, improved information sharing in TTIP may be a tall order. The EU is only now in the process of instituting a formal mechanism for coordinated sharing of information on cyber intrusions among its 27 member states. This process would likely have to play out before the EU could contemplate the further step of U.S.-EU information sharing in the aftermath of attacks, the EU official suggested.

On joint policy responses to cyber attacks, observers were also a bit skeptical. On the one hand, the White House is actively considering policy options to "up the ante" on China if it refuses to scale back its economic espionage; options like visa revocations and financial sanctions against Chinese entities, which could have trade implications, are clearly "on the table," they say, and it therefore might make sense to try to bolster cooperative efforts with the EU.

However, the EU official noted that the EU currently does not have a central authority to coordinate efforts with the U.S. in the aftermath of an attack, as this is the prerogative of member states. This could make it more difficult to really make headway on the issue of joint coordination, this official signaled. The two sides already conduct response exercises to mock attacks under a bilateral working group, in which member states participate.

Moreover, the official suggested that a substantive outcome in this area might be "a bit more difficult," partly because companies do not always choose to report security breaches and, when they do, Europe is still in the process of figuring out how this information will be shared among its member states. It is also often hard to know exactly who is behind a given cyber attack, complicating the objective of joint responses, this EU official noted.

Several observers suspected that the U.S. might have more luck looking to advance discussions on joint responses in a forum like the North Atlantic Treaty Organization, which has already started cybersecurity discussions.

The issue of cyber standards and regulations may also come up in TTIP; for instance, the two sides might agree to set up a mechanism to ensure that they stay in close contact on future regulations related to cyber-related issues. Thus far, the U.S. and EU are focused on crafting voluntary "best practices" for companies to follow, but binding regulations could come further down the line, and it would help businesses if they were not divergent, Levinson noted.

This issue was also raised by the Transatlantic Business Council in its comments. "Through TTIP, the U.S. and EU have an opportunity to embrace emerging common cybersecurity standards, incentives and principles that minimize both security threats and any trade-distorting impacts," it wrote. Specifically, it argued that TTIP should incorporate by reference the principles of a global information communications technology statement from 2012.

That statement -- endorsed by the Information Technology and Industry Council, Digital Europe and the Japan Electronics & Information Technology Industries Association -- lists 12 principles, including that governments should develop cybersecurity policies in partnership with the private sector and that cybersecurity policies should be technology-neutral and allow for procurement regardless of the nationality of the technology vendor.

In their comments, many leading business associations -- including the U.S. Chamber of Commerce, National Foreign Trade Council and the National Association of Manufacturers (NAM) -- stressed the importance of using TTIP to bolster protections for trade secrets, which are often stolen through cyberspace. Many associations spoke about the particular importance of using TTIP to promote trade secret protection in third markets.

"Through the TTIP, the United States and the EU should commit to sharing ... best practices with other governments given the scant attention paid by many of them to the protection of trade secrets and the increasing incidences of cyber theft and other misappropriations," NAM wrote in its comments. Similarly, BSA | The Software Alliance urged the two sides to "develop a comprehensive model trade secret protection system that can be promoted globally."

NAM also argued that TTIP "should include a blueprint for effective enforcement mechanisms that reinforce protection and deter bad actors in third countries from using illicitly-obtained information," including through "adequate fines and civil damages." In the Trans-Pacific Partnership talks, USTR has tabled language that would require criminal penalties for government officials that disseminate trade secrets (*Inside U.S. Trade*, March 9, 2012).

Another cyber-related issue that could come up in the forthcoming trans-Atlantic negotiations is the fact that some foreign governments are requiring the disclosure of trade secret information as a condition of licensing or doing business, which was also raised in the NAM comments. The EU official agreed that the two sides might use TTIP to strengthen their commitment to ensuring that third parties do not use cybersecurity as an excuse to erect trade barriers.

If the U.S. and EU do try to forge ahead on cyber issues in TTIP, they will not start from a blank slate.

The two parties established a bilateral dialogue in November 2010 on cybersecurity and cyber crime issues. According to the EU official, this dialogue focuses on issues like responses to cyber intrusions -- including the staging of joint exercises simulating cyber attacks -- ways to work with the private sector on cybersecurity issues, and raising awareness of the importance of cybersecurity measures among private-sector actors.

The Office of the U.S. Trade Representative and the European Commission's international trade arm both declined to make substantive comments for this story. "As we are currently engaged in detailed consultations with Congress and our domestic stakeholders on what our negotiating objectives should be, we cannot comment on the specifics of what a Transatlantic Trade and Investment Partnership agreement would include at this point," a USTR spokeswoman said.