WorldECR

'Don't go too far with Iran,' U.S. tells the World 3

Penalty Spot: United Arab Emirates in focus 7

Thailand moves closer to publishing control list 9

U.S. revises Cuba sanctions regulations to further normalise trade with Cuba 10

Talking export controls with Laura Rockwood 14

Is the AECA really extraterritorial? 17

Update: Iranian Nuclear Procurement Channel 22

Balancing investment liberalisation and national security in China-U.S. relations 27

EU aviation and Iran sanctions: current position 32

ISSUE 44. OCTOBER 2015
www.WorldECR.com

‘Make room for space.’ EU amends Russia sanctions in light of industry concerns

The European Union has made changes to its restrictive measures against Russia so as to ensure that European space programmes reliant on Russian satellite launches are not jeopardised by the sanctions regime.

Council Decision (CFSP) 2015/1764 notes that the Council’s Decision 2014/512/CFSP concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine ‘should not affect the European space industry’, and thus:

‘…certain operations concerning specific pyrotechnics referred to in the Common Military List of the European Union, necessary for the use of launchers operated by launch service providers of Member States or established in a Member State, or for the use of launches of space programmes of the Union, its Member States or of the European Space Agency, or for the fuelling of satellites by satellites manufacturers established in a Member State, should be permitted.’

copyright: ESA

Ariane 5 lift-off on flight VA226. Amendments to the EU’s sanctions against Russia aim to protect the EU space industry.

The amended regulation permits some otherwise prohibited exports where they are ‘for use of launchers operated by European launch service providers, or for the use of launches of European space programmes, or for the fuelling of satellites by European satellites manufacturers.’

Reid Whitten of law firm Sheppard Mullin told *WorldECR*:

‘Given that it was only in September that the EU issued a continuation of its export restrictions against Russia, and now the concerns being voiced by [president] Hollande and others over Russia's action in Syria, I think this relatively small export policy adjustment could be termed a “softening”. It has been evident that some European businesses, those with strong ties or a dependence on trade with Russia, have chafed under the EU export restrictions. I think this change, particularly with its requirement that the fuel be used only for EU launches, is a limited concession to the EU aerospace industry that may need certain Russian fuels.’

Clarification welcomed

In late September, the EU Council published clarifications, by way of FAQs, to the existing sanctions regime against Russia. The FAQs cover topics relating to the provision of financial assistance, restrictions on dual-use goods and technology, the definition of ‘specialised floating vessels’ (which does not cover supply vessels such as platform supply vessels, anchor handling tug and supply vessels or emergency response vessels, for the purposes of Regulation 833/2014, financial services, loans and emergency services.

Commenting on the FAQs, Charles De Jager of law firm Crowell & Moring observed that amongst other issues addressed, they ‘clarified points regarding the trade finance exemption.’

According to De Jager, ‘In this context, the exemption is included to ensure legitimate EU trade is not hampered. [With the sanctions up and running,] people have gone back to the EU authorities and asked for better guidance on how to deal with the regulations.’

De Jager believes that the EU’s experience in providing these clarifications will have informed its actions when reviewing the space-related sanctions. ‘The same thing happened here,’ he says. ‘The European space industry told the EU authorities “You didn’t really think [the sanctions] through, they are really impacting our work.”

‘Given proper oversight, there’s no reason why legitimate trade in Europe shouldn’t take place. I see these changes as a necessary refining process of the sanctions as opposed to a loosening of EU policy towards Russia. These changes reflect the realisation that where there are legitimate areas of activity to the EU, there is no need to be overly strict – otherwise Europe would just be shooting itself in the foot.’

The FAQs can be found at: http://europa.eu/newsroom/files/pdf/1_act_part1_v2_en.pdf

Sanctions no bar to ISO development

Number 4 of the EU’s FAQs asks: ‘Is the participation in the ISO standardisation activities prohibited under Article 2a of Regulation (EU) No 833/2014?’

It provides the following answer: ‘No. Participation in the ISO standard development process pursues a legitimate goal and does not imply, per se, violation of EU restrictive measures. Thus, representatives of EU entities are not prevented from continuing their standardisation activities. Considering the nature of standardisation activities, it can be presumed that the transferred technology in the framework of standard-setting activities is compatible with the provisions of Regulation (EU) No 833/2014. Nevertheless, the relevant persons should be called upon to remain vigilant about the type of technology shared in such a context. In case of doubt, the competent authority of the relevant Member State should be contacted for guidance.’

‘Don’t go too far with Iran,’ United States tells the rest of the World

The U.S. State Department has recently cabled a demarche warning foreign governments not to get ahead of themselves in their dealings with the Islamic Republic of Iran.

According to news agency Reuters, the note ‘cautioned against a rush by Western companies to invest in Iran's oil industry and other businesses until the country fully complies with the July nuclear agreement [and]...stressed that sanctions on Iran would not be lifted until the International Atomic Energy Agency verifies that Tehran has complied with the terms of the deal.’

Small steps

Ongoing research by *WorldECR* suggests that while many businesses, financial intermediaries and banks are revisiting their policies *vis a vis* ‘de-risking’ in relation to Iran, they find themselves in a quandary. As one finance industry insider told *WorldECR*: ‘Non-U.S. financial intermediaries are looking at opportunities in Iran. But U.S. banks have been told that they cannot do business with correspondent banks that do business with Iranian banks. And of course, EU companies and banks that have a listing in the U.S. will have to report any transactions with Iran to the SEC. Even if those aren’t in breach [of sanctions] the thought of doing so will probably dampen their enthusiasm for re-entering the Iranian market.’

UK ECO takes on board tech concerns

The UK’s Export Control Organisation (‘ECO’) is to address concerns raised in a report by trade association techUK that the country’s technology industry is disadvantaged by UK export controls. The decision was made public in an open letter from ECO head Edward Bell to techUK director of operations Paul Hide.

The letter states: ‘Firstly, related to Finding 1 in techUK’s report (competitive disadvantage caused by the way the UK implements export controls), ECO will review the system of End User Undertakings to simplify their scope and application to reduce the regulatory burden on UK exporters. A number of stakeholders will be consulted during the review and we would like to invite techUK and ADS to play central consultative roles to ensure the voice of business is fully understood and taken into account.

‘Secondly, related to techUK’s Finding 2 (licensing lead times), ECO will review open general licensing to determine the scope for moving more exports to light touch licensing arrangements, which exporters may register for online for immediate use without End User Undertakings. This would expand the scope of Open General Licences which provide quick access to “off the shelf” licensing cover for a range of exports and destinations. Once again, a number of stakeholders will be consulted during the review and we would like to invite techUK and ADS to play central consultative roles.’

It also said that ECO ‘is making proposals to ministers for the reintroduction of a comprehensive Control List Classification Advice Service. This would provide exporters with one-to-one access to expert advice about how controls apply to their products and services.’

Baker & McKenzie partner Ross Denton told *WorldECR* that Bell’s comments were ‘sensible and reflect what we see in our practice,’ and disagreed with any suggestion that the ECO was merely acquiescing to industry requests for reduced regulation.

Denton added that, in his experience, ‘Businesses actively engaged with the licensing system welcome active enforcement. Exporters who flout licensing obligations have little interest in increased enforcement. The burden (and cost) of licensing always falls on exporters that do comply, and only infrequently does enforcement go against those that do not comply. This is an unfair balance in favour of those that do not comply.’

But he said that on occasion, ‘Licencing officers do not understand the products or the needs of businesses’ altogether and their approach can require business to explain products and their characteristics each time they apply for a licence.

‘There are several elements of the licensing system that can be vastly improved,’ said Denton. ‘For example, consider a software company that needs licensing on a number of different occasions. Whenever they send out an application to the ECO, they are assigned a person who doesn’t know anything about the company or about software. If you had a dedicated licensing official – either for the business or for the sector – the process would be smoother and more productive. [ECO] have talked about implementing such strategies in the past, but it is not an easy issue for ECO, as it would require ECO having the budget to train and retain specialist licensing officers who either know the products of a company, or have deep industry specialisation.’

The letter is at:
http://discuss.bis.gov.uk/focusonenforcement/files/2015/09/Response-to-techUK-report.pdf

The report by techUK is at:
http://www.techuk.org/insights/news/item/3762-techuk-s-report-on-export-controls-published-by-bis

Xi and Obama: consensus on cybercrime?

President Barack Obama and Chinese leader Xi Jinping reached a cordial modus operandi regarding cybersecurity during the latter's recent visit to the United States – or so official statements suggest.

In his concluding statements at a joint press summit on 25 September, President Xi said:

'Confrontation and friction are not made by choice for both sides. During my visit, competent authorities of both countries have reached important consensus on [a] joint fight against cyber-crimes. Both sides agree to step up crime cases, investigation assistance and information-sharing. And both governments will not be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace. And we will establish a high-level joint dialogue mechanism on the fight against cyber-crimes and related issues, and to establish hotline links.'

A White House fact sheet supported Xi's message, noting: 'The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community.'

China and the U.S. have pledged to fight cybercriminals together.

'[W]e will establish a high-level joint dialogue mechanism on the fight against cyber-crimes.'
Xi Jinping

Given the extent of rivalry between the two nations, few observers believe the visit marks the beginning of a mutual 'hands-off' pact. On a posting on the think-tank's website, Brookings Institute expert Richard Bejtlich remarked: 'On balance, the agreement is a step in the right direction. At best, I would expect it to result in a decrease in the digital intrusion pressure applied by Chinese military and intelligence forces against American companies. The Chinese would likely continue pursuing their strategic goals by changing tactics at the human level and operations and the merger and acquisition level. At worst, I expect the agreement to have no effect whatsoever.'

DC-based Steptoe & Johnson partner Stewart Baker told *WorldECR*: 'China and cybersecurity will remain a major issue despite the heavily negotiated sentences about not conducting cyber espionage for commercial gain. Even with the best will in the world, and that isn't assured by any means, President XI has less control over cyberespionage than many people think. There's plenty of what might be called "crony espionage" by PLA generals spying to help out Chinese industry leaders from whom they expect rewards.'

Baker does see a possible positive consequence: 'A more realistic view of the agreement is that it gives companies who are victimised by theft of trade secrets some hope that they can hurt any of their competitors who benefit from the thefts. Companies who think they're targeted for cyberespionage on behalf of Chinese competitors will need to build a strong forensic and legal case. Thanks to this agreement, they'll have somewhere to go once they've built that case.'

Ireland holds Euro1.5bn in frozen funds

The Republic of Ireland's Minister for Finance, Michael Noonan has released figures provided by Ireland's central bank detailing the amount of frozen funds held in Irish banks pursuant to EU sanctions. Money frozen in connection with sanctions on Libya accounts for the vast majority of the total, €1,482,885,723, and funds frozen under the EU's Iran, Al-Qaida, Syria, Liberia, Burma, North Korea, and Somalia sanctions bring the total to €1,485,661,150.

Currently, 36 people and 18 entities are listed on the EU's sanctions on Libya, which include United Nations and Europoean Union designations for those involved in serious human rights abuses or violations of international law in Libya. Several of the listed people are relatives of the late Libyan President Gaddafi.

Maya Lester, europeansanctions.com

The figures in full are at:

http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail2015092200072?opendocument#WRN03250

DOJ pulls u-turn on prosecution of Chinese American academic

The U.S. Department of Justice ('DoJ') has dropped the prosecution of a Chinese American scientist which saw the DoJ initially alleging that the professor of physics – head of department at Pennsylvania's Temple University – was sharing sensitive technology with China. The climb-down has garnered wide publicity, and calls for the DoJ to apologise to Xi Xiaoxing, who was arrested at gunpoint by federal agents earlier this year. As reporting by the *New York Times* notes, prosecutors initially believed that Dr Xi had shared with scientists in China the blueprints for a device called a 'pocket heater' used in superconductor research. While the technology that Xi was alleged to have sent was not controlled, the sharing of it, authorities believed, was prohibited by Xi's signing of a non-disclosure agreement ('NDA').

Xi's lawyer, Peter Zeidenberg of Arent Fox, told *WorldECR*: 'The [authorities] were wrong about their facts. Their contention was not that it was controlled technology, but, rather, that the sharing of information was prohibited by a NDA, which Prof. Xi had fraudulently induced the seller to enter into. If the technology had been controlled, that would have undoubtedly led to additional charges. But the fact is, the technology that Professor Xi shared was unrelated to the technology covered by the NDA.'

After his May arrest, Xi was placed under restrictions that prevented him from continuing research. Zeidenberg made his case by arranging for affidavits by scientists – including a co-inventor of the pocket heater – who swore that the technology shared by Xi was not what prosecutors had originally believed. On 11 September, the government formally moved for all charges against Xi to be dropped.

Xi Xiaoxing, professor at Pennsylvania's Temple University

Tech sector put on alert

Zeidenberg believes current U.S. sensitivities about China suggest it's likely that similar scenarios will be played out in future. 'It just goes to shows how aggressive the government is in making these cases, particularly in relation to China,' said Zeidenberg. 'It means that individuals involved in tech transfers of whatever nature must be extremely aware of the scrutiny that they're going to be under. It isn't enough to say that technology isn't uncontrolled. Unfortunately, the fact that you're not in violation of the law doesn't mean that you're out of the woods.'

Zeidenberg added: 'The fact is that university science departments collaborate routinely with counterparts in other countries, including China, and though this is beneficial to the United States, the government views it as harmful [while] the fact that the U.S. government itself often invites information sharing with China sends very mixed messages. This is a very difficult area from a compliance perspective.'

Enforcement: BIS and Commerce issue denial orders

The U.S. Bureau of Industry and Security ('BIS') has announced the imposition of denials of export privileges against two individuals and three companies 'involved in a conspiracy to illegally export and re-export web monitoring and controlling equipment and software to Syria, including to the state-run Syrian Telecommunications Establishment (STE). The illegally exported and re-exported items are controlled by the Commerce Department for national security and anti-terrorism reasons and as encryption items.'

BIS said that it was imposing 'a denial order for five years against Aiman Ammar and for six years against Rashid Albuni, both of the United Arab Emirates,' and that their companies, Engineering Construction and Contracting and Advanced Technology Solutions, located in Damascus, Syria, each received seven-year denials, while a third company, iT-Wave FZCO of Dubai, U.A.E., received a four-year denial. Financial penalties were also imposed.

'The settlement announced today results from the aggressive law enforcement effort to prevent the Syrian government from acquiring technology that can repress the Syrian people,' said Under Secretary of Commerce for Industry and Security, Eric L. Hirschhorn.

TDO renewed

Meanwhile, the U.S. Department of Commerce has renewed a temporary denial order ('TDO') denying export privileges to a U.S. company, Flider Electronics (doing business as Trident International Corporation), which, Commerce says, has continued to seek to flout the Export Administration Regulations ('EAR') despite being served with the TDO in March.

Explaining the decision, Commerce Assistant Secretary David Mills said that the original order, valid for 180 days, denied privileges to Trident and to company officials Pavel and Gennadiy Flider. The Office of Export Enforcement ('OEE'), he said, had presented evidence of exports to Russia, via transhipment through Finland or Estonia, involving false statements and other 'evasive actions' intended to camouflage the exports' final destinations, end-users and end uses. The exported items included U.S. items on the Commerce Control List. Subsequently, and despite the TDO, Pavel has, Mills said, 'repeatedly sought to order or buy items subject to the EAR from a U.S.-based electronics distributor from whom Trident had previously purchased items for export.'

Mills said that renewal of the TDO was 'necessary to avoid imminent violation of the EAR, based upon the evidence presented by the OEE of deliberate and evasive conduct both pre- and post-issuance of the TDO,' and that accordingly, U.S. persons should not deal with Trident or the Fliders in any EAR-related transaction.

U.S. senator introduces bill to tighten North Korea sanctions

Colorado Senator Cory Gardner, chair of the of the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, has introduced a new bill that would further tighten sanctions on North Korea.

According to Gardner, the North Korea Sanctions and Policy Enhancement Act of 2015 'includes broad new sanctions against individuals involved in North Korea's nuclear program and proliferation activities, as well as officials involved in censoring the regime's continued human rights abuses.'

New legislation, he said, would provide 'several corrections to United States policy and strategy related to North Korea' and would state 'that it is the policy of the United States to vigorously pursue sanctions against the North Korean government in order to peacefully disarm the North Korean regime. It would require the President to submit a strategy to counter North Korean cyber-related attacks and impose U.S. sanctions on cybercriminals.'

Senator Gardner's bill reflects a desire for 'a stronger, more focused policy on North Korea'.

Inter alia, the bill would 'codify two executive orders released in 2015 authorizing sanctions against entities undermining U.S. national and economic security in cyberspace. Further, it would require a report by the State Department identifying human rights abusers in North Korea and a report on the North Korean regime's political prison camps.'

Gardner said of his decision to propose the measures: 'We need a stronger, more focused policy on North Korea, and if the Administration is unwilling to provide it, Congress must act. The new sanctions within this legislation would apply the pressure required to change North Korea's behavior, and would mandate that the United States finally have a unified strategy for dealing with North Korean cyber attacks. We can't go any longer without a serious plan to deal with this threat. It's time to get serious.'

FBI, Moldovans and others on the nuclear trail

In early October, various media reported an Associated Press ('AP') investigation into how attempts by organised crime groups in Eastern Europe to sell ingredients for a so-called 'dirty bomb' to terrorists including 'Islamic State' have been foiled by local police in collaboration with the FBI. The investigation found that much of the material being sold originated in Russia, and was possibly made available in collusion with rogue elements of the Russian intelligence community.

A BBC 'timeline' drawn from the AP report showed a number of successes on behalf of the authorities:

- 2010: 1.8kg of Uranium-238 seized in Chisinau when three people tried to sell it for €9m;
- 2011: Six detained for trying sell 1kg of weapons-grade Uranium-235 for €32m. They said they also had access to plutonium.
- 2014: Smugglers allegedly tried to sell 200g of Uranium-235 from Russia to undercover security agents for $1.6m; 1.5kg of Uranium-235 seized close to Moldovan border in Ukraine.
- 2015: Undercover agent bought ampoule of Caesium-135; materials contaminated with Caesium-137 found in central Chisinau.

Daniel Salisbury, a researcher at the Centre for Science and Security Studies within the Department of War Studies at King's College London, told *WorldECR*:

'The AP report outlines four cases in Moldova where "smugglers" have sought to sell nuclear and radioactive materials over the past five years. This is obviously concerning – in the most recent case, in 2015, the individual trying to sell the radiological material was seeking a buyer from Islamic State.'

According to Salisbury, 'The material in this case – different isotopes of Caesium – was not suitable for use in a nuclear weapon. In fact, the Caesium "purchased" by the undercover agent was not suitable for use in an improvised dirty bomb – although more suitable Caesium-137 was also supposedly being offered by the seller.'

Salisbury said that since the end of the Cold War, 'Many cases have been seen in former Soviet Union countries, many of which held large amounts of these materials, and where the security at facilities storing them was often lax.'

He added: 'Much effort has been put into trying to secure these materials through installing improved physical protection measures at facilities, and efforts to build a nuclear security culture amongst employees. That the FBI was involved in the recent case in Moldova suggests that there is ongoing collaboration between the authorities in many of these countries and those in the U.S. and elsewhere in tackling this important issue.'

PENALTY SPOT

For various reasons, **The United Arab Emirates** found popularity with proliferators as a place through which to divert controlled items and technologies. But, as Ryan Lynch Cathie, notes, the UAE has responded by tightening up its controls and their enforcement.

The United Arab Emirates ('UAE') is one of the few countries in the Middle East region to have adopted a comprehensive export control system.

Throughout the 1990s and early 2000s, the UAE had been a target of proliferators of WMD- and military-related items. The UAE's liberal trade policies, proximity to and longstanding trade relations with Iran, heavy transit and transshipment trade volumes, and numerous Free Trade Zones ('FTZs') were exploited regularly by those seeking to divert strategic goods and technologies to countries and/or entities of concern. With both international pressure and technical support, the UAE decided to enact Federal Law No. 13 of 2007 (as amended by Federal Law No. 12 of 2008 'Concerning Commodities Subject to Import and Export Control'), in order to more effectively regulate trade in 'strategic commodities', i.e. dual-use and military-related goods and technologies.

Federal Law No. 13 (as amended) requires individuals and entities to seek a licence for the export (including intangible transfers of technology), re-export, transit, transshipment, and brokering of strategic commodities. Further, UAE legislation contains a 'catch-all' provision that requires traders to seek a licence (for non-listed items) when the individual knows or is informed (by the UAE Committee for Goods and Materials Subject to Import and Export Control) that the commodity will or may be used, in whole or in part, in the development, handling, production, operation, maintenance or storage of weapons of mass destruction ('WMD') or their means of delivery. (Federal Law No. 13, Article 8)

The Law also prescribes a range of administrative and criminal penalties for non-compliance, as follows:

Federal Law No. 13, article 7: A licence may be revoked if the licence holder fails to meet any of the terms or conditions set forth in the licence.

Federal Law No. 13, article 16: Individuals or entities that violate the export, re-export, transit, trans-shipment, brokering, and catch-all provisions of the law are subject to criminal penalties:

> 'Whoever violates the provisions of Articles 8 and 10 (i.e. With respect to the unauthorized export, re-export, brokering, transit and transshipment) – of this Law shall be sentenced to imprisonment for a period not less than one year and a fine not less than AED 50,000 (US$13,500) and not more than AED 500,000 (US$135,000) or to one of these penalties. The penalty shall be doubled in the case of recidivism. In case of conviction the court may decide the confiscation of the commodities subject of the crime.'

The failure to maintain records as specified by the law (article 14) or the failure to provide the Committee with any requested documentation or information is also subject to sanction under the law. Violators

> 'shall be sentenced to imprisonment for a period not in excess of one year and for fine not less than AED 10,000 (US$2,700) and not in excess of AED 50,000 (US$13,500) or to one of these penalties, the penalty shall be doubled in case of recidivism.'

The Law also maintains specific penalties for breaches of the confidentiality provisions (article 15) or for submitting false or misleading documentation. In such cases, violators

> 'shall be sentenced to imprisonment for a period not less than one year and to a fine not less than AED 50,000 (US$13,500) and not more than AED 500,000 (US$135,000) or to one of these penalties.'

Note: Pursuant to article 16(4) of Federal Law No. 13,

> 'the infliction of the penalties provided for in this law does not prejudice any more severe penalties provided for in any other law.'

In addition to Federal Law No. 13, other UAE legislation such as Federal Law No. 6 of 2009 'Regarding the Peaceful Uses of Nuclear Energy', Federal Law No. 40 of 2006 'Regarding the Prohibition of Innovating, Producing, Storing, and Using Chemical Weapons', and Federal Law No. 5 of 2013 'On Weapons, Ammunition, Explosives and Military Equipment' regulate the licensing, handling, use and control of these types of goods and materials, and include specific penalties for violations.

Federal Law No. 6 of 2009 'Regarding the Peaceful Uses of Nuclear Energy' maintains the following penalty provisions:

- Article 62: anyone who conducts regulated activities without a licence, intentionally fails to comply with the law, intentionally alters destroys or otherwise suppresses documentation or information, or submits false information shall be penalised by imprisonment for a period of not more than one year

Links and notes

[1] An official English language translation of Federal Law No. 5 is unavailable. Other penalties within the law are outlined in Articles 58-73 of the Arabic version, available at: http://rakpp.rak.ae/ar/Pages/%D9%85%D8%B1%D8%B3%D9%88%D9%85-%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86-5-%D9%84%D8%B3%D9%86%D8%A9-2013-%D8%A8%D8%B4%D8%A3%D9%86-%D8%A7%D9%84%D8%A3%D8%B3%D9%84%D8%AD%D8%A9-%D9%88%D8%A7%D9%84%D8%B0%D8%AE%D8%A7%D8%A6%D8%B1-%D9%88%D8%A7%D9%84%D9%85%D8%AA%D9%81%D8%AC%D8%B1%D8%A7%D8%AA-%D9%88%D8%A7%D9%84%D8%B9%D8%AA%D8%A7%D8%AF-%D8%A7%D9%84%D8%B9%D8%B3%D9%83%D8%B1%D9%8A.aspx

[2] Federal Law No. 40 of 2006 is not available in English. The Arabic version of the law can be found at: http://theuaelaw.com/vb/archive/index.php/t-151.html

[3] 'Export control and combating terror financing,' Embassy of the United Arab Emirates in the United States, 2015, http://www.uae-embassy.org/business-trade/trade-export/export-control-and-combating-terror-financing

[4] 'Court to re-issue spying charges for Buaschor to March 30,' Al Khaleej, 3 March 2015, http://www.alkhaleej.ae/alkhaleej/page/f0fadc0a-3156-4a24-b109-669ea9bb1f4c

and a fine not less than AED 500,000 (US$135,000) and not more than AED 50 million (US$13.5 million) or by one of these two penalties.

- Article 63: The unlawful possession you transfer or disposal of a nuclear material shall be punished with a temporary jail sentence in a fine of not less than AED 2 million (US$540,000) and not more than AED 50 million (US$13.5 million) or buy one of those two penalties.

Federal Law No. 5 of 2013 'On Weapons, Ammunition, Explosives and Military Equipment' outlines a range of penalties related to trade in firearms, ammunition and explosives [1] that include:

- Article 56: a licence to transfer firearms, ammunition, and explosives may be revoked for any violation of the law or its implementing regulations.
- Article 60: the unauthorised import, export, or transit of firearms, ammunition, and explosives is punishable by a term of imprisonment of not less than six months and a fine of not less than AED 15,000 (US$4,050)
- Article 71: UAE authorities may confiscate goods and the means of transport and cancel a licence when a violation of the law has occurred.
- Article 72: Penalties may be doubled in the case of recidivism.

Federal Law No. 40 of 2006 'Regarding the Prohibition of Innovating, Producing, Storing, and Using Chemical Weapons' (as amended in 2008), articles 12-17[2] details violations punishable:

- Article 12: failure to provide requested information or providing false or inaccurate information to the Committee is punishable by imprisonment and a fine not less than AED 20,000 (US$5,400) or both.
- Article 14: the unauthorised export, transport, storage, manufacture, trade, possession, or use of toxic chemicals subject to the law is punishable by imprisonment and/or a fine of not less than AED 100,000 (US$27,000) and not more than AED 500,000 (US$135,000). Any person who violates any provision of article 8 (i.e. unauthorised export, transport, storage, manufacture, trade, possession, or use of toxic chemicals) shall have the chemicals in question confiscated by UAE authorities.

Federal Law No. 7 of 2014 'On Terrorist Offences' designates penalties for terrorism financing and transfers of conventional and non-conventional weapons which are used for terrorism purposes.

- Federal Law No. 7, article 29: Terrorism financing – Life imprisonment or temporary imprisonment for no less than 10 years shall be imposed [on whoever] 'acquires, takes, manages, invests, possesses, transmits, transfers, deposits, keeps, uses or disposes of funds or carries out any commercial or financial bank transaction although aware that all or part of such funds are collected as a result of a terrorist offence, owned by a terrorist organisation or intended for the financing of a terrorist organisation, person or offence.' (Also see Federal Law No. 7, articles 30-33)
- Federal Law No. 7, article 7(1): 'Life imprisonment shall be imposed on whoever manufactures, collects, prepares, supplies, imports, exports, enters to or exists from the State, acquires, possesses or disposes of non-conventional weapons or transfer or attempts to transfer such weapons by post or any means of transport for a terrorist purpose.'

To date, evidence of effective strategic trade control enforcement has been somewhat mixed in the UAE. In 2008, shortly after Federal Law No. 13 entered into force, UAE authorities seized numerous shipments bound for Iran, some of which included cargo containing dual-use aluminum sheets, titanium, high-speed computers, and CNC machine tools.[3] Two years later, UAE authorities shut down more than 40 international and local companies involved in money-laundering and proliferation activities. Since then, strategic trade enforcement actions in the UAE have occurred with less frequency. Nonetheless, there is evidence that the UAE continues to enforce its controls and is prosecuting individuals for unauthorised trade in strategic goods. In March 2015, an individual was prosecuted in the UAE Federal Supreme Court for violations of Federal Law No. 13. The individual is accused of illegally importing a military chipset and audio analyser from the U.S. by falsifying the end-use and end-user documentation, and subsequently re-exporting the equipment to an unauthorised end-user in Syria.[4]

Ryan Lynch Cathie is Managing Director, Products & Innovation, at SECURUS Strategic Trade Solutions, LLC.

ryan.cathie@securustrade.com

EU

EU Court annuls sanctions on the Belarus football club Dinamo Minsk and Yury Chyzh

By Maya Lester, Brick Court Chambers

www.europeansanctions.com

The European Court has annulled the inclusion of Yury Chyzh & companies linked with him in the Triple group, and the Belarus football club Dinamo Minsk, on the EU's sanctions relating to Belarus.

The EU first imposed restrictive measures (an arms embargo, asset freeze and travel ban) in 2006 on President Lukashenko and Belarusian officials said to be responsible for serious human rights violations, whose activities seriously undermine democracy or the rule of law in Belarus, or who benefit from or support the Lukashenko regime.

Yury Chyzh was included for providing financial support to the regime through his company Triple, and FA Dinamo Minsk (which was founded in 1927 and continued in exile after the occupation of Minsk in 1941) was included for being owned by Triple. The General Court has held that being a leading businessman in Belarus is not enough on its own to show that Mr Chyzh provided financial support to the regime, and the Council put forward no evidence that he does, nor that the concessions he had won were not won through merit. The Court said that to have held otherwise would have exceeded the objective of the EU legislature, and interestingly the Court also applied the principle of legal certainty to sanctions listings. Since Mr Chyzh's designation was not justified, nor was that of Triple or the other companies said to be owned by him, nor that of FA Dinamo Minsk. The Court did not suspend operation of the annulment, and ordered the Council to pay costs.

Maya Lester acts for all of the applicants.

Links and notes

Case T-275/12
http://curia.europa.eu/juris/document/document.jsf?text=&docid=169161&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=134449

Case T-276/12
http://curia.europa.eu/juris/document/document.jsf?text=&docid=169165&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=134524

THAILAND

Thailand moves closer to publishing control list

By Jay Nash, Securus Trade

www.securustrade.com

After a long wait, we may be getting somewhat closer to knowing the precise set of items that will be on Thailand's dual-use export control list. According to the *Bangkok Post* and several other media sources, the Thailand Ministry of Commerce ('MOC') has 'announced' the list of items that will be used as the basis for Thailand's dual-use export control system. The 3 October *Bangkok Post* article and other reports cite Thailand Commerce Minister Apiradi Tantraporn as the source of this latest information. The reports state that the list will cover 1,230 dual-use items, and give 1 January 2018 as the date when the list and Thailand's dual-use export controls will enter into force. Media reports in Thai indicate that the Ministry of Commerce made a formal announcement regarding the dual-use control list on 22 September.

A search of both the Thai and English versions of the MOC (and its Department of Foreign Trade ('DFT') website did not produce a published announcement of any kind. However, the DFT did post an image on its Facebook Timeline on 2 October with the tag (loosely translated to English): 'Management measures for the trade of dual-use goods of Thailand'.

Since the Thai cabinet adopted in principle a draft MOC notification on dual-use export controls earlier this year (and even long before that), many have been eager to see what Thailand's dual-use control list would comprise. All indications have been that Thailand's dual-use control list will be based on the EU's List of Dual-Use Items, though, at 1,230 items, Thailand's dual-use list would have almost 500 fewer items than the EU list (which is reported to cover closer to 1,700 total items).

One possible explanation for the difference is that items on the EU list that already are trade-controlled by other Thai government agencies pursuant to existing legislation and lists are those 500 or so items that will not end up on the MOC's dual-use list. If that is indeed the case, the question remains whether and how the trade controls and licensing requirements and procedures for the two 'groups' of items will differ. For now, one thing may be certain: we will have a good 24-plus months to figure it out and prepare accordingly.

Links and notes

http://www.bangkokpost.com/news/general/716488/new-curbs-put-on-dual-use-weapon-item

http://www.naewna.com/business/181850

https://m.facebook.com/story.php?story_fbid=956251241117076&substory_index=0&id=682203435188526

U.S.A.

U.S. revises Cuba sanctions regulations to further normalise trade with Cuba

By Michael E. Zolandz, Peter G. Feldman, Kenyon Weaver and Jason M. Silverman

www.dentons.com

On 18 September 2015, the U.S. Department of Treasury and U.S. Department of Commerce released significant revisions to the U.S. embargo on Cuba, as set out in the Cuban Assets Control Regulations ('CACR') and the Export Administration Regulations ('EAR'). These changes will loosen a number of trade sanctions currently in effect. Among other things, the revised regulations permit U.S. businesses to establish operations in Cuba in certain circumstances, relax controls on travel and remittances to Cuba, authorise commercial and financial transactions with Cuban nationals outside of Cuba, and expand opportunities for U.S. firms to provide telecommunications services to Cuba. The changes took effect on 21 September 2015.

The revised Cuba sanctions regime

The U.S. has long had one of the most extensive sanctions regimes with respect to Cuba. Many of the prohibitions set out in the CACR apply not only to U.S. individuals and entities, but also to the overseas subsidiaries of U.S. entities.[1] The CACR has moreover prohibited transactions with Cuban nationals even where they are located outside of Cuba. The revisions to the CACR and EAR roll back many of these prohibitions.

The key changes set out in the revised CACR and EAR are as follows:

Establishing a presence and opening accounts in Cuba

Persons subject to U.S. jurisdiction who are now authorised to engage in trade with Cuba will also now be able to establish a physical presence in Cuba and open bank accounts in Cuban banks. Thus, persons who have been authorised under the revised CACR to trade with Cuba will also now be able to open an office, hire Cuban nationals and open a Cuban bank account. They will also be permitted to conduct marketing activities in connection with their presence in Cuba. Companies that may establish a physical presence in Cuba under this new rule include companies facilitating permitted exports (including certain consumer communications devices, construction supplies and equipment to the private sector, agricultural equipment to the private sector, and supplies, equipment and tools for private sector entrepreneurs); as well as companies involved in mail, parcel and cargo transportation; telecommunications services (see below); news; travel services; and entities engaging in authorised educational and religious activities.

Transactions with Cuban nationals outside of Cuba

All persons subject to U.S. jurisdiction will now be permitted to provide goods and services to Cuban nationals located outside of Cuba. Under the revised CACR, moreover, banking institutions – whether or not subject to U.S. jurisdiction – will also be allowed to open, maintain and close bank accounts for these Cuban nationals without risk of U.S. sanctions.

Financial transactions

The revised CACR loosens restrictions on sending money to or from Cuban nationals, whether located in or outside of Cuba. Cuban nationals may now make remittances to persons subject to U.S. jurisdiction, and vice-versa, without a cap on the amount, so long as neither the sender nor receiver is a prohibited official of the government of Cuba or the Cuban Communist Party. The revised CACR furthermore

eliminates the limitation on remittances that may be carried on one's person back to Cuba. Where remittances are currently blocked (such as because the remittances were over the limitation), the revised CACR establishes a general licence that would allow these to be unblocked. Cuban nationals lawfully present in the United States (in a non-immigrant status, or pursuant to other non-immigrant travel authorisation) may now also open and maintain bank accounts without having to close them prior to their departure.

Expansion of telecommunications services

The revised CACR also rolls back prohibitions in the telecommunications and Internet sector, expanding the list of services now permitted to be exported or re-exported to Cuba with regard to consumer communications devices under the EAR, including with respect to software design, business consulting and IT management services. The CACR also now authorises training related to the installation, repair or replacement of those permitted items. As noted above, persons subject to U.S. jurisdiction who are engaged in providing telecommunications and Internet-based services may now establish a presence and open a bank account in Cuba. The revised CACR also authorises these persons to enter into licence agreements and to market services, and permits the import of Cuban-origin mobile applications and the employment of Cuban nationals to develop such applications.

Persons subject to U.S. jurisdiction who are engaged in providing telecommunications and Internet-based services may now establish a presence and open a bank account in Cuba.

Travel

New general licences will be available for direct travel between the U.S. and Cuba, and for travel for close relatives to visit or accompany authorised travellers on a number of different grounds, such as educational activities, journalistic activity, professional research and religious activities, as well as activities related to humanitarian projects and activities of private foundations or certain research or educational institutes. Notably, however, the U.S. continues to prohibit general tourism travel to Cuba.

Exports

The EAR licence exception Support for the Cuban People ('SCP'), which was created in January 2015, has been expanded.[2] Exception SCP is now adapted to facilitate the various trade opportunities allowed under the revised CACR. Accordingly, SCP will now authorise a range of new exports and re-exports, including exports and re-exports of items to Cuba for use in establishing, maintaining and

operating a physical presence in Cuba by authorised end-users, i.e., persons providing permitted telecommunications or Internet-based services, travel services, etc. Previously, the SCP was limited to sales and donations transactions; it will now be expanded to other types of transactions, such as leases and loans.

The EAR will also be amended to facilitate export of certain items relating to civil aviation and vessels, as well as the temporary sojourn in Cuba of certain vessels. Licence exception Aircraft, Vessels and Spacecraft ('AVS'), which allows export of equipment, spare parts for permanent use on a vessel or aircraft, and ship and plane stores, will now be available for use to Cuba, provided any items exported are designated as EAR 99 or controlled only for anti-terrorism ('AT') reasons. The Bureau of Industry and Security ('BIS') will also now permit use of the exception for temporary sojourn in Cuba of cargo and commercial passenger vessels, as well as recreational vessels if used in connection with travel authorised by the Office of Foreign Assets Control ('OFAC').

In addition, BIS will now evaluate on a case-by-case basis licence applications to Cuba relating to improving the safety of civil aviation, such as for aircraft parts and components relating to safety, weather observation stations, airport safety equipment and commodities used for security screening of passengers. Until now, BIS has applied a policy of denial to such licence applications.

Other

Building on President Obama's December 2014 announcement and the January 2015 changes, the revised CACR also loosens prohibitions in the following areas:

- **Legal advice** The revised CACR permits persons subject to U.S. jurisdiction to provide – and be paid for – the provision of legal services to Cuba and Cuban nationals, with regard to legal advice on U.S. law, so long as the advice is not in furtherance of transactions violating the CACR.
- **Mail and cargo** The revised CACR allows persons subject to U.S. jurisdiction to provide mail and cargo services, as well as remittance forwarding services, for authorised services.
- **Educational activities** The revised CACR expands the scope of authorised educational activities, including standardised testing services and Internet-based courses to Cuban nationals, and also authorises academic exchanges and joint non-commercial academic research between U.S. and Cuban universities.
- **Air ambulances** The revised CACR authorises air ambulances to travel to and from Cuba to evacuate individuals requiring medical care.
- **Gifts** The revised CACR will allow goods from Cuba or Cuban-origin goods that are intended as gifts to be sent to the United States, under certain circumstances.
- **Humanitarian projects** The revised CACR expands humanitarian projects to include disaster relief and historical preservation missions.
- **Cuban official missions** The revised CACR authorises fund transfers on behalf of official missions of the government of Cuba in the United States.
- **New section to permit transactions 'ordinarily incident' to a licensed transaction** The revised CACR adds a new section 515.521 to authorise any transaction ordinarily incident to a licensed transaction and necessary to give effect to such licensed transaction. In its new guidance, OFAC provides the example of a payment made using an online payment platform for authorised transactions.

Implications

With its historical ties, close proximity to U.S. shores, and U.S.$68 billion economy, Cuba may prove to be a significant market for a number of U.S. businesses. Under the revised CACR, this market is now more open to U.S. citizens and residents, U.S. businesses as well as U.S. businesses' overseas subsidiaries. Certain companies that are permitted to export items or services to Cuba now have a path by which they might establish a greater commercial foothold in that country. The telecommunications, banking and travel sectors in particular benefit from the revisions to the CACR. In addition, it is not unreasonable to expect that the expanded authorisations of financial transactions with Cuba may make it easier for U.S. persons or entities lawfully conducting business in or traveling to Cuba to access U.S. accounts – an issue that has reportedly presented challenges to U.S. travellers.

At the same time, the general commercial embargo remains in effect, and any transaction not authorised under the CACR or a general licence will require a specific licence from OFAC. Thus, for example, while travel to Cuba may now be significantly easier, travellers subject to U.S. jurisdiction must still ensure their travel is valid under the CACR or general licence, and ordinary tourism remains banned. This is reflected in the revised CACR section authorising travel to Cuba for market research, commercial marketing, sales negotiation, accompanied delivery, installation or servicing, which still retains its caveat: 'provided that the traveler's schedule of activities does not include free time or recreation in excess of that consistent with a full-time schedule.'

Although the changes to the CACR and EAR are significant, the long-term trajectory of U.S.-Cuba trade normalisation and corresponding trade relief remains uncertain. This trajectory will likely depend as much on the next U.S. president as the current one, and the topic of Cuba sanctions can be expected to surface in the coming months as the various U.S. presidential candidates establish their positions on foreign policy. Moreover, a number of Cuba sanctions are pursuant to statute. It will take an act of Congress to reverse these prohibitions. Businesses entering the Cuban market should therefore be prepared to navigate a shifting regulatory landscape.

Links and notes

[1] The CACR defines 'persons subject to the jurisdiction of the United States' to include not only U.S. citizen or resident individuals (wherever located), persons physically in the U.S. and entities organised under U.S. law, but also any non-U.S. entity owned or controlled by U.S. individuals or U.S.-organised entities.

[2] https://www.federalregister.gov/articles/2015/01/16/2015-00590/cuba-providing-support-for-the-cuban-people

U.S.A.

DDTC agrees that the public domain prior approval requirement is unreasonable

By Christopher B. Stagg, Stagg P.C

www.staggpc.com

On 3 June 2015, the Directorate of Defense Trade Controls ('DDTC') issued a proposed rule to amend the public domain exclusion within ITAR § 120.11 to include a prior government approval requirement. In proposing this revision, DDTC made a curious statement in the preamble that prior government approval is not a new requirement and that the proposed revision is merely 'a more explicit statement of the ITAR's requirement that one must seek and receive a license or other authorization [to put information into the public domain].'

This is a curious statement because DDTC has previously stated to the federal courts that reading ITAR § 120.11 to impose a prior approval requirement is 'by far the most unreasonable interpretation of the provision' and also 'one that people of ordinary intelligence are least likely to assume is the case.' Accordingly, DDTC confirmed to the federal courts in 1996 that there is no prior approval requirement to put information into the public domain. The federal court case where DDTC made these statements is *Bernstein v Department of State*.

These are highly damaging statements by DDTC. Not only does DDTC's statement unequivocally maintain that there is no prior approval requirement, but it also establishes that the position DDTC now takes is admittedly 'by far the most unreasonable interpretation of the provision' and 'that people of ordinary intelligence are least likely to assume is the case'.

Since DDTC concedes that 'people of ordinary intelligence' would not read the public domain exclusion to impose a prior approval requirement, this raises a due process claim under the Fifth Amendment that DDTC's new interpretation is unconstitutionally vague. The legal standard for a due process vagueness claim is whether the law would give fair notice to persons of ordinary intelligence of the legal requirements. Also, in laws that concern speech covered by the First Amendment, the federal courts impose an even higher standard by requiring that the law has even greater clarity.

Here, DDTC concedes that such persons would not have notice.

DDTC's statements in the court case also confirm that it has a long-standing practice of not requiring prior government approval to put information into the public domain. In changing its practice, it is well-established law that a regulatory agency must (1) acknowledge it is departing from prior practice and (2) explain the reason for the departure. The failure by a regulatory agency to follow these requirements raises due process issues. For instance, without an agency following these procedural requirements in changing its position, courts could not know whether a regulatory agency acted erroneously.

Here, DDTC fails both requirements. Instead of recognising it as departing from prior practice, DDTC simply asserts that this is not a new requirement. Yet, the regulatory history of the public domain exclusion and DDTC's own admissions to the federal courts clearly evidence that this is incorrect. Since DDTC failed to acknowledge it is departing from prior practice, it also failed to fulfil the second well-established requirement of explaining the reason for its departure.

Talking export controls with LAURA ROCKWOOD

Laura Rockwood was appointed as Executive Director of the Vienna Centre for Disarmament and Non-Proliferation as of 1 June 2015. She was most recently a Senior Research Fellow at Harvard University's Kennedy School Belfer Center, managing the Atom Project. Ms Rockwood retired in November 2013 from the International Atomic Energy Agency ('IAEA') as the Section Head for Non-Proliferation and Policy Making in the Office of Legal Affairs, where she had served since 1985. Prior to working for the IAEA, she was employed by the U.S. Department of Energy as a trial attorney in radiation injury cases, and as counsel in general legal matters.

WorldECR: Tell us about the creation of the Vienna Center for Disarmament and Non-Proliferation ('VCDNP'), and the role that it plays. What is it about Vienna that makes it a good location for the Center?

Laura Rockwood: The initiative to establish a dedicated non-governmental platform for independent debate, research, outreach, education and training related to disarmament and non-proliferation was first announced at the 2010 (Treaty on the Non-Proliferation of Nuclear Weapons) NPT Review Conference by the Austrian Foreign Minister. With its 'critical mass' of nuclear expertise, and as the home to a number of international organisations dedicated to addressing nuclear non-proliferation and disarmament, including the IAEA (International Atomic Energy Agency), the CTBTO (Comprehensive Nuclear-Test-Ban Treaty Organisation), and others, Vienna was a logical place to create such an entity.

The Center, operated by the James Martin Center for Nonproliferation Studies ('CNS') at the Middlebury Institute of International Studies at Monterey, was also envisioned as a place for results-oriented discussion among the many stakeholders: national governments, international organisations, academia and civil society.

With the launch of the VCDNP in 2011, disarmament and non-proliferation education and outreach enjoyed a significant boost. The VCDNP offers training for diplomats, practitioners and journalists, as well as public seminars featuring some of the top experts on nuclear non-proliferation, disarmament and international security. The Center also hosts expert workshops, Track 1.5 and Track 2 meetings and international conferences, where we create a safe haven for open and frank off-the-record discussions among government officials, academics and other experts.

WorldECR: There is, of course, consensus that non-proliferation is a good thing. But have nuclear-armed nations lost the appetite for disarmament? One of the policy recommendations emerging from last year's Vienna Conference on the Humanitarian Impact of Nuclear Weapons was that 'all states parties to the NPT … renew their commitment to the urgent and full implementation of existing obligations under Article VI' , but the meaning and desirability of that commitment does not draw consensus (while the nuclear-free Middle East initiative appears to have been removed from the agenda).

Laura Rockwood: There is definitely a sense of frustration at the resistance of the nuclear-weapon states to take additional actions in the direction of disarmament. On the other hand, the nuclear-weapon states feel as though not enough credit has been given for the steps they have taken. I think that a large part of the problem is that there hasn't been much dialogue in the sense of real communication between these two positions; there have been exchanges of positions, but no real effort to come to grips with the legitimate concerns of the other side.

The Middle East is a separate issue from the overall disarmament and humanitarian impact debate. I don't think it's off the table, but there's a lot of weariness after the NPT Review Conference.

WorldECR: It looks now as though the P5+1 and Iran negotiations have been successful, though the deal has doubters and detractors. You support the Iran deal. Could you tell us, from a technical (and/or political) perspective, what gives you confidence in the outcome of the negotiations?

Laura Rockwood: Yes, I do support the Iran deal. The arrangement establishes a highly intrusive inspection regime that would make it virtually impossible for Iran to develop a nuclear weapons programme without detection. We are far better off today with a limited nuclear programme highly constrained by the JCPOA (Joint Comprehensive Plan of Action) than we were – or would be – without the deal and an unrestrained programme in Iran. Agreement on the JCPOA also reduces the risk of another military conflict in the region, and creates the opportunity for the reintegration of Iran into the global community. There are certainly critics of the deal – those who would argue, for example, that loosening sanctions would free up money for Iran to spend on other military ventures. But I don't think all of these issues can be resolved at once.

WorldECR: Does the success of the Iran negotiations create a re-alignment in priorities for the non-proliferation agenda?

Laura Rockwood: With the resolution of the Iranian nuclear issue, the most immediate non-proliferation threat is that of North Korea. It seems to be an intractable problem. Perhaps the success of the Iran deal will inspire a greater willingness on the part of North Korea to re-engage in discussions about its nuclear programme. Another looming threat today is that of a non-state actor like Islamic State achieving – through illicit procurement networks – any part of a nuclear programme. While that is considered a nuclear security issue (since it relates to non-state actors) rather than a non-proliferation issue (which is generally used to refer

to proliferation by a state), I believe it is a more real and immediate threat at this point than another state 'going rogue'.

WorldECR: One of the striking elements of the P5+1 negotiations appeared to be the close working relationship between John Kerry and Sergei Lavrov at a time when relations between the U.S. and Russia have been at a post-Cold War low. Can that working relationship be maintained in support of other pressing global issues?

Laura Rockwood: The fact that the U.S. and the Russian Federation were able to maintain a unified front in the context of the Iran negotiations demonstrates that the two countries still share common concerns, and can actually cooperate to address those concerns, at least with regard to the threat of horizontal spread of nuclear weapons in non-nuclear-weapon states. Where I think the cooling relationship has had an immediate and negative impact is on the willingness of the two countries to engage in any further bilateral arms control or disarmament activities. It is critical at this stage that channels remain open – if not on a formal basis, at least on what is referred to as the Track 1.5 or Track 2 basis – to ensure that security issues – not just nuclear security but all aspects of security – can continue to be resolved without resorting to military conflict.

WorldECR: You have written about the development of the 'state-level concept'. This is a controversial issue – the debate around which has been shaped by the discovery of the Iraq nuclear programme in the 1990s, the events leading up to the invasion of Iraq, and other episodes. You are an exponent of an interpretation of the IAEA's mandate that holds that the agency has the duty not only to verify that what a member state has declared about its nuclear capacity is correct, but to evaluate all 'safeguards-relevant information' about a state, and – as you have written – 'tailoring safeguards to fit the state concerned.' Why does this approach make some nuclear nations – and proliferation experts – uncomfortable?

Laura Rockwood: The IAEA's authority – and, yes, obligation – to verify the declarations of non-nuclear-weapon states under its comprehensive safeguards agreements are correct and complete is clear from the terms of those agreements. That authority has been confirmed on numerous occasions by the member states of the IAEA.

Likewise, the IAEA's approach of looking at the state as a whole – rather than focusing on individual facilities – and taking into account all safeguards-relevant information about a state, with a view to optimising the implementation of safeguards in that state – has been endorsed by its membership since the IAEA began doing so in the late 1990s. Nothing about that approach is new. Unfortunately, the high turnover in the diplomatic community creates the opportunity for the lessons of history to be lost. I believe much of the recent concerns were attributable to a lack of awareness of that history.

That isn't to say that the concerns expressed by some states during the discussions on the state-level concept were not genuine. A number of states wished for reassurances that the judgments by the IAEA would not be based on subjective factors, and that it would draw conclusions only on the basis of information it has been able to verify independently. These concerns, and others raised by the states, were addressed in detail by the IAEA Secretariat. However, I also believe that some of the challenges can be attributed to external political circumstances unrelated to safeguards that capitalised on that lack of awareness.

WorldECR: Do you think that the nuclear industry understands its role – and obligations – in non-proliferation efforts and takes them seriously? Do you see any causes for concern in terms of industry practice – or, conversely, stellar examples of best practice?

Laura Rockwood: I would really like to see more buy-in from industry in the area of non-proliferation, including in the areas of safeguards and export controls. I have already seen developments in that direction and support them whole-heartedly. As a matter of fact, I have just been attending a conference in which one of the key issues discussed in the non-proliferation community was how better to engage the industry in these matters. I think the best way of achieving that is to demonstrate that good non-proliferation practices are not just good policy, but that they are good for the bottom line as well.

'I would really like to see more buy-in from industry in the area of non-proliferation, including in the areas of safeguards and export controls.'

Laura Rockwood

WorldECR: What is the role of business in the non-proliferation effort? Does it bear too much of the brunt of the responsibility for enforcement on behalf of overstretched authorities?

Laura Rockwood: Do they bear a responsibility and does it sometimes appear to be an onerous one? No doubt. But industry is the first line of defence against illicit acquisition of nuclear technology and equipment. They are best placed to detect suspicious or false inquiries and to share that information with the state authorities. I think there should be more industry-to-industry exchanges on the value of effective export controls. They are also in an excellent position to advocate for good safeguards, appreciating that, while they themselves may not be a proliferation problem, the IAEA will be obliged to implement the same safeguards in similar facilities in other countries.

WorldECR: Are you optimistic that global non-proliferation efforts – i.e. the collective sum of multilateral organisations, unilateral initiatives and agencies, civil society groups and industry associations – is fit to meet the needs of this century?

Laura Rockwood: Absolutely. I'm basically an optimist anyway. But I believe that the global community – states, international organisations, civil society, academia and industry – has and can continue to work together to weave the warp and woof of this fabric of non-proliferation tightly enough to prevent the rise of yet another nuclear armed state – and, worse still, a nuclear-armed non-state actor. However, we cannot afford to be complacent.

Unsung heroes

'First Libya was the enemy, then it was our friend, then it was the enemy, then it was our friend again – and our compliance plan had to take into account all these changes!' So said a participant at the recent *WorldECR* Forum in London, illustrating very neatly how rapidly, and sometimes with seeming inconsistency, high-level policy and value judgements impact on the bottom line of business. Not that she was begrudging the need to be ethical in business – far from it. But she reminded us that what is 'ethical' is a political judgement as much as it is a moral one.

The truth of this is also demonstrated by the recent announcement that the UK is pulling out of a bid to provide training to the Saudi ministry of justice. Though it hasn't said quite so much, it has baulked at the prospect of assisting a judicial system that includes flogging, decapitation, stoning, crucifixion and amputation amongst the penalties it is entitled to carry out. Meanwhile, UK Trade and Investment claims on its website that the country 'has a strong historic relationship with Saudi Arabia. The Kingdom is our largest trading partner in the Middle East…Over 6,000 UK firms actively export goods to Saudi Arabia.' But where is the cut off between 'good' and 'bad trade'?

At the Forum, it emerged that the European Commission is looking at a new consideration that would inform export control policy: human security. This would marry elements of international security with human rights considerations. And in Sweden, we heard, there are proposals to prohibit military sales to countries that are insufficiently democratic.

Companies deserve clear guidance from government as to what they are allowed to export to whom.

On the face of it, this makes sense. But who is to decide who is sufficiently democratic to deserve exports? And do some criteria outweigh others? Would a country with fully-fledged democratic institutions but which treats a particular sector of its society badly make for a better trading partner than an autocratic regime with an otherwise strong record on human rights?

Companies deserve clear guidance from government as to what they are allowed to export to whom. In the absence of such a steer, they're obliged to anticipate political wind-shifts and public perceptions – and exercise ethical discretion on their own account. It's a tough call – and often enough, much of its weigh falls on the shoulders of the compliance function.

Those in that profession that I regularly converse with are humane, highly ethical, intelligent, and all too conscious of the need to make decisions that are grounded in law, bear the scrutiny of the NGO community and the press, whilst also enabling the interests of their colleagues and shareholders. These aren't easy tasks, and they're unlikely to get easier soon. I say: hats off to those who juggle those competing imperatives day by day – they're doing an invaluable job.

Tom Blass, October 2015
TNB@worldecr.com

Is the Arms Export Control Act really extraterritorial?

That the jurisdiction of ITAR extends beyond the United States is generally accepted as being above question. But Michael Bell believes that U.S. Supreme Court rulings on extraterritoriality makes this assertion debatable.

The U.S. International Traffic in Arms Regulations ('ITAR') are interpreted as being extraterritorial ('XT') in scope. The regulations 'follow the part'[1] in the sense that U.S.-origin U.S. Munitions List defence articles and defence services are treated as subject to U.S. jurisdiction wherever they are in the world and throughout their lives[2]. Consequently, foreign persons outside the U.S. are required to comply with the ITAR and are subject to sanctions under U.S. law if they fail to do so[3].

The ITAR currently gives effect to Section 38 of the Arms Export Control Act ('AECA') (22 USC 2778), which authorises the President to control the export and import of defence articles and defence services, a power delegated ultimately to the Directorate of Defense Trade Controls ('DDTC') of the Department of State[4].

This article considers whether the AECA is extra-territorial in scope and in consequence supports the extra-territorial basis of the ITAR. (It is a fundamental principle of constitutional law that regulations cannot be broader in scope than the primary legislation from which they are derived.) For the purposes of the article, 'extra-territoriality' is defined as the assertion of jurisdiction over foreign persons outside the U.S. The article takes advantage of recent developments in the brokering regulation (Part 129 of the ITAR) to illuminate the discussion. The analysis is confined exclusively to the interpretation of U.S. law; the views of U.S. allies are not addressed[5].

XT and the Brokering Amendment

In 1996, the AECA was amended to enable control to be exercised over brokers[6]. The ITAR was updated accordingly with a new Part 129. Part 129.2(b) stated that the regulation applied (but was not limited) to activities by U.S. persons located inside or outside of the USA or by 'foreign persons subject to US jurisdiction'. Similarly, Part 129.3(a) placed a requirement to register on any U.S. person, wherever located, and any foreign person located in the United States 'or otherwise subject to the jurisdiction of the United States'.

Foreign persons outside the U.S. are required to comply with the ITAR and are subject to sanctions under U.S. law if they fail to do so

The DDTC issued no guidance on the interpretation of 'otherwise subject to US jurisdiction', or indeed on any other aspect of Part 129. Contemporary commentators opined that the language should be interpreted in terms of foreign brokers 'having a sufficient nexus with the US based on the activities in question', or 'employed by US companies or having an unrelated business in the US'[7].

With the passage of time, however, it became increasingly clear that the DDTC asserted jurisdiction over foreign brokers outside the U.S. even if their only connection with the U.S. was with involvement in brokering U.S.-origin defence articles or defence services, i.e., jurisdiction 'followed the part', as elsewhere in the ITAR. The stage was set for a decade-long war of attrition between the DDTC and informed legal opinion as to the extra-territorial scope of the AECA brokering amendment.

In 2003, the DDTC informed the U.S. Congress that it intended to review Part 129 in the light of experience. In 2009, a new draft was put to the Defense Trade Advisory Group ('DTAG') which replaced the language of 'otherwise subject to US jurisdiction' with the more specific statement that 'brokering activities include any such activities by...any foreign person located outside the US who engages in brokering activities involving a US-origin defense article or defense service'[8]. The same language was included in draft text published as a Federal Register Notice ('FRN') in December 2011[9].

DDTC had also imposed, in May 2011, a consent agreement on BAE Systems plc, a foreign person outside the United States, for 2,588 alleged violations of the ITAR brokering regulations involving U.S. origin defence articles and defence services[10].

Meanwhile, successive statements of legal opinion, in the case of *US v. Yakou*[11], in an unsolicited input in February 2008 to the Department of State's legal adviser by the American Bar Association ('ABA')[12], and by a commentary on the December 2011 FRN from the Section of International Law ('SIL') of the ABA[13], argued that application of standard principles of statutory construction, as confirmed by the U.S. Supreme Court, did not permit an extra-territorial interpretation of the AECA brokering amendment.

Under such principles, 'Congress legislates with a presumption against extraterritoriality. Federal laws apply only within the territorial jurisdiction of the United States unless Congress provides "affirmative evidence" to the contrary. This intention must be "clearly expressed"'[14]. The AECA brokering amendment provided no such evidence.

The ABA's was only one of a large number of forcefully expressed criticisms of the December 2011 FRN. As a result, the DDTC, in a text trailered with the DTAG in December 2012[15] and published, slightly modified, as an interim final FRN in August 2013[16], finally abandoned its efforts to extend Part 129 jurisdiction to foreign persons outside the U.S., with the exception of foreign persons 'owned or controlled' by U.S. persons.

While the DDTC did not go so far as to admit error, it observed laconically that where 'the recommendations [of commentators] were in conformance with the requirements for brokering as set forth in the AECA…the Department has made amendments accordingly'.

XT and the AECA

As stated above, the statutory authority to regulate traffic in arms is derived from S38 of the Arms Export Control Act (22 USC 2778) (see box 'Arms Export Control Act' for pertinent part).

The question of XT reach of the AECA was addressed and confirmed in the judgment of *US v Evans*[17] in 1987 (see '*Annex: US v Evans*' at the end of this article for pertinent part).

The first point to note is that S2778 clearly does not satisfy the principles of statutory construction for XT, as adumbrated in successive legal opinions on the brokering rule. There is no 'affirmative evidence' or 'clearly expressed' intention. What is affirmatively and clearly expressed is that the section applies (only) to 'exports and imports'. *Evans (1987)* of course precedes the Supreme Court rulings (1991, 1993) cited by *Yakou* and the ABA[18].

That said, the arguments in *Evans* must be considered on their merits. They are in brief twofold: first, that the act applies to 'any person', unlimited in scope, and second, that the act is 'international in focus'. *Evans* also cites 22 USC 2753, which requires end-users to seek U.S. government ('USG') authority before re-exporting. These points are considered successively.

Evans points out that S2778(c) penalties apply to 'any person who willfully violates any provision of this section'; 'The underscored language is not confined to persons acting in the United States or "persons of the United States."' This is not a convincing argument, for the following reasons:

- 'any person' who is not subject to the jurisdiction of the AECA cannot violate its provisions, hence the argument is circular[19];
- S38(b) states that 'every person … who engages in the business of manufacturing, exporting, or importing any defense articles or defense services designated by the President under subsection (a)(1) of this section shall register…' It is obvious that 'every person' is not intended to have universal application, since foreign arms manufacturers cannot be required to register in the U.S.[20]

Similarly the AECA brokering amendment requires 'every person who engages in the business of brokering activities' to register. The DDTC has now conceded in its latest FRN that the jurisdiction of the brokering regulation is limited to U.S. persons, foreign persons within the U.S. and foreign persons owned or controlled by U.S. persons. There seems to be no good reason why the jurisdiction of other parts of S2778 should not be similarly interpreted.

The 'international character' of the AECA is demonstrated, according to *Evans*, by references in the act to 'world peace and the security and foreign policy of the United States'. But there is no need to infer from these references an XT reach for the act. This is not the place for a detailed account of the legislative history of the AECA[21]. Suffice it to say that the Congress was primarily motivated by concerns over the international impact of inadequately regulated U.S. arms exports, both by the Administration and by private companies. Hence, the reference in S2778(a)(1) to the control of 'exports and imports of defense articles and defense services' can and should be read at face value and no more[22]. Moreover, the Supreme Court rulings make it clear that the test of XT is not whether it is reasonable but

Arms Export Control Act

§2778. Control of arms exports and imports

(a) Presidential control of exports and imports of defense articles and services, guidance of policy, etc.; designation of United States Munitions List; issuance of export licenses; negotiations information

(1) In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.

(2) Decisions on issuing export licenses under this section shall take into account whether the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements.

(3) In exercising the authorities conferred by this section, the President may require that any defense article or defense service be sold under this chapter as a condition of its eligibility for export, and may require that persons engaged in the negotiation for the export of defense articles and services keep the President fully and currently informed of the progress and future prospects of such negotiations.

(b) Registration and licensing requirements for manufacturers, exporters, or importers of designated defense articles and defense services

(1)(A)(i) As prescribed in regulations issued under this section, every person (other than an officer or employee of the United States Government acting in an official capacity) who engages in the business of manufacturing, exporting, or importing any defense articles or defense services designated by the President under subsection (a)(1) of this section shall register with the United States Government agency charged with the administration of this section, and shall pay a registration fee which shall be prescribed by such regulations

[Brokering amendment deleted]

(c) Criminal violations; punishment

Any person who willfully violates any provision of this section, section 2779 of this title, a treaty referred to in subsection (j)(1)(C)(i), or any rule or regulation issued under this section or section 2779 of this title, including any rule or regulation issued to implement or enforce a treaty referred to in subsection (j)(1)(C)(i) or an implementing arrangement pursuant to such treaty, or who willfully, in a registration or license application or required report, makes any untrue statement of a material fact or omits to state a material fact required to be stated therein or necessary to make the statements therein not misleading, shall upon conviction be fined for each violation not more than $1,000,000 or imprisoned not more than 20 years, or both.

whether it is explicit. As noted above, the AECA fails this test[23].

Evans's citation of 22 USC 2753 appears at first sight to be telling, since 2753(a)(2) prohibits end-users from *re-exporting* items sold under this section without prior USG authority. There are, however, two points to be made about this.

First, S2753 refers specifically to transactions by the USG (and not commercial exports by U.S. private companies). It is true that the substance of S2753 has been incorporated into the ITAR, as 123.9, but it is questionable whether this is a legitimate use of discretion, especially given that S2778 nowhere refers to transactions under S2753.

Secondly, however, even if retransfer restrictions have been legitimately imposed on commercial exports, it is also questionable whether a requirement for non-transfer and use certificates (ie DSP-83s) prior to export constitutes an assertion of XT jurisdiction. There is evidence on this score in the disclaimer made by the British government when submitting DSP-83s, which reads in part:

> 'However, signature is without prejudice to Her Majesty's Government's position on the validity of what it believes to be the US Government's claim to extra-territoriality. Her Majesty's Government notes that the US Government does not view the DSP-83 assurance requirement as involving a claim to extra-territoriality'. (my underlining)[24].

The USG's position would appear to be reasonable, since such end-use certificates are more in the nature of bilateral agreements, on the lines of MOUs, than assertions of XT jurisdiction. It is worth noting here that other nations impose similar requirements for end-user certificates under legislation which does not purport to be XT.

Finally, the reference in ITAR Part 127.3(c) to 'all persons abroad subject to US jurisdiction'[25] needs to be reinterpreted in the light of the clarification of the same language in ITAR Part 129. In Part 129 as reissued, those parties subject to U.S. jurisdiction have now been specifically defined as: U.S. persons wherever located, foreign persons within the U.S., and foreign persons owned or controlled by U.S. persons. It would be illogical to claim that jurisdiction 'follows the part' in Part 127 if it has been accepted that it does not do so in Part 129.

Conclusions

The ITAR relies on an XT interpretation of the AECA. This allows the DDTC to assert jurisdiction over ITAR-controlled exports overseas, including foreign end-items incorporating U.S.-origin hardware or derived from U.S.-origin technical data or defence services, and over foreign persons overseas involved with them. Application of the standard U.S. principles of statutory construction, as determined by the Supreme Court and accepted in the context of the ITAR brokering regulation, shows, however, that there is no 'affirmative evidence' for XT scope for the AECA, nor is such an intention 'clearly expressed'. The AECA thus fails the test of XT set by the Supreme Court. Consequently, in asserting XT jurisdiction, the ITAR goes beyond the scope permitted by the AECA.

Links and notes

1 See *Little et al*, 2006, which supports an XT interpretation of the AECA.

2 This jurisdiction is held to extend to the re-export or retransfer of foreign end-items into which U.S.-origin defence articles, however minor, are incorporated (the so-called 'see-through' rule), or which are derived from U.S.-origin technical data or defence services (sometimes known as 'tainting'). See ITAR 123.9(b)(1) and 124.8(5).

3 See ITAR 127.1(c): All persons abroad subject to U.S. jurisdiction who obtain temporary or permanent custody of a defense article exported from the United States or produced under an agreement described in part 124 of this subchapter, and irrespective of the number of intermediate transfers, are bound by the regulations of this subchapter in the same manner and to the same extent as the original owner or transferor.

4 U.S. arms export controls in their modern form date from the 1935 Neutrality Act, which introduced comprehensive licensing of exports, a requirement for arms manufacturers, exporters and importers to register, a supervisory Office of Arms and Munitions Controls in the DoS, and a pamphlet, catchily titled 'International Traffic in Arms-Laws and Regulations Administered by the Secretary of State Governing the International Traffic in Arms, Ammunition and Munitions of War, and other Implements of War'. See Joseph C Green, 'Supervising the American Traffic in Arms', Foreign Affairs July 1937. Green was the first Chief of the Office.

5 America's allies have had difficulties with the assertion of XT jurisdiction in trade matters and have on occasion taken countermeasures, such as the UK Protection of Trading Interests Act 1980 or EU Council Reg 2271/96 (the 'blocking statute'), though neither has been applied to ITAR. The UK government rejects ITAR XT jurisdiction in principle but complies in practice. See UK MOD Acquisition System Guidance (formerly Acquisition Operational Framework), Procurement from the USA, para 99: 'HMG does not recognise the right of USG to impose controls in this way [ie on retransfers], as this involves XT rights and is therefore an infringement of UK sovereignty'.

6 Section 2778(b)(1)(A)(ii) of the AECA. 3. References in Capito, 2007, page 308

7 DTAG November 2009 Brokering Draft

8 FR/2011/76FR78578

9 BAE Systems plc Consent Agreement

10 393 Fed 231 (DC Cir 2005) at *US v Yakou*. Yakou was charged with brokering patrol boats for the Saddam regime in Iraq. The case hinged on whether Yakou's 'green card' status was still valid, and thus whether he was a 'U.S. person'. The courts determined that Yakou was no longer a 'U.S. person'. The DDTC saved something from the wreckage by successfully appealing that the correct interpretation of 'otherwise subject to U.S. jurisdiction' was not at issue.

11 ABA Feb 2008

12 FRN Brokering Comments, page 143

13 Id. Citations from *EEOC v ARAMCO* 1991, *Sale v Haitian Centers Council Inc* 1993,omitted

14 DTAG December 2012 Brokering Draft

15 FR/2013/78FR52680

16 667 F Supp 974. Evans and his co-defendants were accused of re-selling to Iran U.S.-origin defence articles originally sold to Israel.

17 See fn 13. *Yakou* cites *Evans* but dismisses it as irrelevant

18 Syntactically, the *Evans* interpretation demands a comma between 'any person' and 'who'.

19 Similar 'every person' language occurs in the 1935 Neutrality Act, where XT reach is clearly not intended.

20 There is a useful summary of the background to, and negotiating history of, the AECA in Warren and Logan 1977

21 The ITAR distinguishes between 'export' (120.17), and 'reexport or retransfer' (120.19).

22 See also 1981 Department of Justice Memorandum Constitutionality of the Proposed Revision of the ITAR, fn 5, which, discussing the need to control the export of technical data enabling a foreign enterprise to develop 'technical capacity', comments that 'that capacity is created on foreign soil, beyond the legislative jurisdiction of the United States' (my underlining)

23 Annex C to UKG document referenced in footnote 4.

24 See footnote 2 above

Michael Bell is an independent export control consultant based in the United Kingdom. He was previously Group Export Controls Consultant at BAE Systems, and has held roles in the UK Ministry of Defence and NATO.

mjvbell@inweb.co.uk

Annex: *U.S. v Evans*

United States District Court,
S.D. New York.

UNITED STATES of America
v.
Samuel EVANS; Guriel Eisenberg; Rafael Israel Eisenberg; William Northrup; Avraham Bar'Am; Nico Minardos; Alfred Flearmoy; Hermann Moll; Ralph Kopka; Hans Bihn; Isaac Hebroni; John Delaroque; Bernard Veillot; B.I.T. Company, Import, Export, and Metals Limited; Dergo Establishment; Flear Holdings Incorporated S.A.; International Procurement and Sales, Inc. and Vianar Anstalt, Defendants.

No. 86 Crim. 384 (LBS).
July 10, 1987.

B. Principles of Extraterritoriality as the Basis for Jurisdiction

Defendants contend that jurisdiction of the United States over this case – where many of the alleged criminal acts took place outside the United States and many of the defendants otherwise had little connection to the United States – is inappropriate because 'not reasonable.' *See Restatement (Second) of Foreign Relations Law* § 403 (Tent. Draft No. 7, 1986) ('*Restatement Dr. 7*') (state may not exercise jurisdiction to proscribe law with respect to activities having connections with other states where unreasonable). Thus, we first address the contours of Congress' power to legislate against the crimes charged in the indictment as defined by international principles of extraterritoriality.

The United States Constitution does not bar extraterritorial application of the penal laws, and numerous cases have upheld the authority of the United States to enact and enforce criminal laws proscribing acts outside the United States that have adverse effects inside the United States. *See, e.g., United States v. King,* 552 F.2d 833 (9th Cir.1976), *cert. denied,* 430 U.S. 966, 97 S.Ct. 1646, 52 L.Ed.2d 357 (1977), and cases cited therein; *Restatement (Second) of Foreign Relations Law* § 402(1)(C) (Tent. Draft No. 6, 1985) ('*Restatement Dr. 6*'). Two principles of extraterritorial jurisdiction recognized under international law are applicable here: the effects or 'objective territoriality' principle and the 'protective' principle. *See, e.g., United States v. Pizzarusso,* 388 F.2d 8 (2d Cir.), *cert. denied,* 392 U.S. 936, 88 S.Ct. 2306, 20 L.Ed.2d 1395 (1968).

[6] The effects principle recognizes that '[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a state in punishing the cause of the harm as if he had been present at the effect....' *Strassheim v. Daly,* 221 U.S. 280, 285, 31 S.Ct. 558, 560, 55 L.Ed. 735 (1911); see also *United States v. Egan,* 501 F.Supp. 1252, 1257 (S.D.N.Y.1980); *Restatement Dr. 6, supra,* at § 402(1)(C). The related protective principle imparts jurisdiction when actions have a potentially adverse effect upon the security or governmental functions of a sovereignty. See, e.g., *Pizzarusso,* 388 F.2d at 10–11; *Restatement Dr. 6, supra,* at § 402(3). The Restatement 'takes the position that a state may exercise jurisdiction [under these circumstances] when the effect or intended effect is substantial and the exercise of jurisdiction is reasonable....' *Restatement Dr. 6, supra,* at § 402 comment d.

[7] Furthermore, although cases are rare, international law permits jurisdiction under these theories even if the act or conspiracy at issue is thwarted before ill effects are actually felt in the target state. *Restatement Dr. 6, supra,* at § 402 comment d; s*ee,* e.g., *United States v. Brown,* 549 F.2d 954, 956–57 (4th Cir.), *cert. denied,* 430 U.S. 949, 97 S.Ct. 1590, 51 L.Ed.2d 798 (1977). For that matter, jurisdiction may be proper even if no acts were committed in that state, especially where the statute does not require proof of an overt act. *See, e.g., United States v. Ricardo,* 619 F.2d 1124 (5th Cir.), *cert. denied,* 449 U.S. 1063, 101 S.Ct. 789, 66 L.Ed.2d 607 (1980); *United States v. Fernandez,* 496 F.2d 1294 (5th Cir.1974); *Pizzarusso,* 388 F.2d at 11.

[8] It would clearly have been a reasonable exercise of jurisdiction for Congress to have anticipated that the Arms Export Control Act would be applied to persons and events outside of its borders. The Reporters' Notes to the Seventh Tentative Draft of the *Restatement on Foreign Relations Law* provides that 'it is more plausible to interpret a statute of the United States as having reach beyond the nation's territory when it is international in focus ... than when it has a primarily domestic focus....' *Id.* at n. 2. In this case, defendants are charged, *inter alia,* with conspiring to present, and in several cases actually presenting, false documents to the United States in order to obtain approval to ship United States arms to Iran in violation of the Arms Export Control Act. This statute, by its terms, is inherently international in scope. Under both the effects and protective principles, the United States has jurisdiction to legislate in order to protect itself from this type of fraud, irrespective of whether the party making the false representation, or conspiring to do the same, is located within United States borders, and regardless of whether the conspiracy is averted before effects are actually felt in the United States

[11] Revisiting the relevant statutory language in considering the argument that AECA does not apply to persons acting abroad, we note that section 2778(c) provides that 'any *person* who willfully violates section 2778 or the regulations issued [thereunder] ... shall upon conviction be fined not more than $100,000 or imprisoned not more than two years, or both.' 22 U.S.C. § 2778(c) (emphasis added). The underscored language is not confined to persons acting in the United States or 'persons of the United States.' A literal interpretation of that language suggests that section 2778(c) encompasses foreign persons who violate the statute and the implementing regulations. Furthermore, section 2778(a)(1) states rather broadly that: '[i]n furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and export of defense articles and defense services....' Although the quoted sentence continues, as the Eisenbergs highlight, by authorizing the President 'to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services,' nothing in the statutory language or legislative history reflects a congressional intent to limit the President's authority to establish regulations which control the transfer of American-made weapons after they are exported directly from the United States. As noted earlier, the legislative history

reflects an intent to control the international flow of armaments. See Senate Committee on Foreign Relations, International Security Assistance and Arms Export Control Act of 1976–1977, S.Rep.No. 876, 94th Cong., 2d Sess. 8 (1976). It would seem to be entirely consistent with this statutory purpose, which is largely repeated in the statute itself at 22 U.S.C. § 2778(a)(1), to seek to control the world-wide transfer of American-made weapons once they leave United States borders.

Other circumstances indicate that the statute is not intended to limit itself to the control of the original export of American defense articles. Section 2753, discussed previously, expressly provides for restrictions on the resale abroad of American-made weapons without prior United States approval. More pertinent to this indictment, the regulations promulgated pursuant to section 2778 reflect an intent to attach restrictions to the transfer of the commodities in question, and to exert this control by imposing requirements on persons who control those commodities after they leave the United States. For example, the resale and transfer regulations referred to in Count One of the indictment state that:

The written approval of the Department of State must be obtained before reselling, diverting, transferring, transshipping, or disposing of a defense article in any country other than the country of ultimate designation as stated on the export license, or on the shipper's export declaration....

22 C.F.R. § 123.9(a). A statement of this requirement must appear at the time of initial export on the shipper's export declaration, the bill of lading, and the invoice. See 22 C.F.R. §§ 123.9(a) and (b). Furthermore, section 127.1(b) of the regulations, which is also referred to in Count One, provides that:

All persons abroad subject to U.S. jurisdiction who obtain temporary custody of defense articles exported from the United States ... and irrespective of the number of intermediate transfers, are bound by the regulations of this subchapter in the same manner and to the same extent as the original owner-transferor.

The regulations thus clearly evidence an intent to control the world-wide flow of American-made weapons by reaching 'persons abroad' who obtain 'temporary custody of a defense article exported from the United States' without regard to the number of 'intermediate transfers.' While 'temporary custody' is not specifically defined in 22 C.F.R. § 127.1(b), the type of control over the destination of the weapons allegedly to be transferred in this case would seem to be included within the appropriate definition. The indictment states in the methods and means section that the Eisenbergs 'would obtain' the articles to be transferred and 'through the defendant B.I.T. COMPANY, would sell them to Galaxy Trade, Inc. for Iran.' See Count One at 4–D. Under this scenario, the obligation to seek and obtain the United States approval for any transfer would thus arise. Similarly, the original transferor would have been bound to seek and obtain the United States approval for the export. The regulations thus ensure that in all cases, the written approval of the Department of State is to be obtained prior to the export or resale of regulated defense articles. *See e.g.,* 22 C.F.R. §§ 123.1, 123.9(a), 123.10(d).

The Iranian Nuclear Procurement Channel: the most complex part of the JCPOA?

The JCPOA includes measures aimed to ensure that single- and dual-use items of nuclear relevance cannot be diverted to any clandestine nuclear programme in Iran nor stockpiled. This updated article presents an overview of how these mechanisms will operate in practice. Ian J. Stewart explains how it should work.

This is an update of the article first published on the WorldECR *website in July. The main changes in this article relate to the adoption of Security Council Resolution 2231, which endorses the JCPOA and changes the terms of the existing embargo on Iranian imports of arms and missile technology.*

On 14 July 2015, the E3+3 reached an historic agreement with Iran, known as the Joint Comprehensive Plan of Action ('JCPOA'), over the future of the country's much-disputed nuclear programme.[1] A week later, the UN Security Council adopted resolution 2231 and added provisions to control the export to Iran of arms and missiles over the duration of the JCPOA. The agreement, which should come into force in the first half of 2016 on 'implementation day', will lock in various measures that are intended to ensure that Iran cannot produce nuclear weapons without such an effort being detected in good time (thus deterring 'breakout' scenarios) and provides Iran, in turn, with much-needed sanctions relief.

The JCPOA includes measures intended to ensure that single and dual-use goods of nuclear relevance cannot be diverted to support any clandestine nuclear programme in Iran, and that Iran cannot unduly stockpile such goods for nuclear end uses in the future. These measures form what the plan calls the 'Procurement Channel', which will be operationalised through a Procurement Working Group ('PWG') of the Joint Commission. Iran has committed to ensure that all procurement of nuclear-relevant goods – whether for nuclear end uses or civil end uses – will be procured through this mechanism. This is a somewhat unique mechanism, which raises numerous operational and political questions.[2] It should be noted that there continue to be numerous unanswered questions about the Procurement Working Group in particular (Albright et al).

It is important to note that while the Procurement Channel is for nuclear-relevant goods, many of the items that Iran will have to procure through it have industrial and commercial uses, including in the petrochemical sector. The Procurement Channel will thus be relevant to many firms seeking to re-engage with Iran in the wake of the agreement and is likely to be a dominant feature of trade with Iran over the next decade. Moreover, the agreement places a substantial compliance burden on the service sectors and on exporting states – much more so than is usual for trade control arrangements.

It is important to note that while the Procurement Channel is for nuclear-relevant goods, many of the items that Iran will have to procure through it have industrial and commercial uses.

The Procurement Channel

The channel was first publicly mentioned in an earlier version of the July agreement, in April 2015, which contained no specifics about what the Procurement Channel was or how it would function.[3] The JCPOA goes considerably further, specifying how the procurement will function and what goods will pass through it. UN Security Council Resolution 2231 goes further still, describing a permits-based system that will apply to exports of arms and missiles.

In terms of the scope of the Procurement Channel, the relevant paragraphs are 6.1.1 and 6.1.2 of Annex IV of the JCPOA:[4]

> 6.1.1 the supply, sale or transfer directly or indirectly from their territories, or by their nationals or using their flag vessels or aircraft to, or for the use in or benefit of, Iran, and whether or not originating in their territories, of all items, materials, equipment, goods and technology set out in INFCIRC/254/Rev.12/Part 1, and, if the end-use will be for Iran's nuclear programme set out in this JCPOA or other non-nuclear civilian end-use, all items, materials, equipment, goods and technology set out in INFCIRC/254/Rev.9/Part 2 (or the most recent version of these documents as updated by the Security Council), as well as any further items if the relevant State determines that they could contribute to activities inconsistent with the JCPOA; and,
>
> 6.1.2. the provision to Iran of any technical assistance or training, financial assistance, investment, brokering or other services related to the supply, sale, transfer, manufacture, or use of the items, materials, equipment, goods and technology described in subparagraph (a) above;

What is controlled?

In practice, there are three main categories of goods that will routinely be referred to the PWG. These are Nuclear Suppliers Group ('NSG') 'Trigger List' items, NSG dual-use items, and non-listed items with a

nuclear utility (akin to 'catch-all'). These are taken in turn. Additionally, as a result of Resolution 2231, three further categories of goods will require authorisation directly from the UN Security Council, although these additional measures will be eliminated after a period of five or eight years. The first category is arms. The second category is missile technology falling on the Missile Technology Control Regime category 1 list (single use) or category 2 (dual-use) items.

Trigger List goods

Trigger List goods are typically identifiable as items with a clear nuclear fuel cycle utility. They include nuclear reactors, complete centrifuges, and other items that are 'specially designed or modified' for a nuclear end use. There is in fact an internationally recognised list of these items, and it is this list that is recognised by the JCPOA. Typically, these items do not have other commercial uses, although there are niche specialist end uses for some Trigger List items, such as heavy water (deuterium oxide), which has uses in the oil industry as well as certain specialist scientific applications.

According to the text of the JCPOA, Trigger List exports will be reviewed by states, the PWG, and the International Atomic Energy Agency ('IAEA') in order to ensure that they are used for stated end uses. It should be noted that the export of technology for light water reactors will not be referred to the PWG. Instead, states must simply notify the UN Security Council of the export. As a result, there will likely be few exports to Iran that fall into this category for review by the PWG.

NSG dual-use goods

The JPCOA requires that proposed exports of NSG-controlled dual-use goods be referred to the Procurement Channel (unless the export is for light water reactors as noted above). The NSG dual-use list includes manufacturing equipment, parts and components that can be used in or to make nuclear-relevant technologies but that can also be used for other industrial and commercial applications.

Many goods captured by the NSG dual-use list can be used for petrochemical and aerospace applications (for example, bellows-sealed values, vacuum pressure transducers, carbon fibre, and filament winding equipment). As such, it is likely that that many exports destined to nominally industrial (rather than nuclear) end uses will be referred to the PWG.

As discussed further below, the exporting state or the PWG can request that end-use verification be undertaken to confirm that the goods have not been diverted to nuclear end uses. In practice, this will require access to non-nuclear sites.

Non-listed goods

Since UN Security Council sanctions were first adopted against Iran's nuclear programme in 2006, the majority of cases reported to the UN's Iran Sanctions Panel of Experts have related to goods not listed by the NSG's Trigger List or dual-use list. This highlights that Iran has required – and will continue to require – non-listed items for its nuclear fuel cycle. As such, it has been necessary to include provisions on non-listed goods in the JCPOA.

The JCPOA provides states with an option to refer cases to the Procurement Channel should they believe that the export of the goods is relevant to the JCPOA.

In practice, the JCPOA provides states with an option to refer cases to the Procurement Channel should they believe that the export of the goods is relevant to the JCPOA. This is loosely the equivalent of the 'catch-all mechanism' that has been included in previous UN Security Council sanctions resolutions, and is also implemented by many states as part of their export control regulations. It should be noted that this mechanism in the JCPOA does differ from traditional catch-all controls, however: in particular, it seems unlikely that non-listed goods destined for Iran's declared nuclear programme would be blocked by the PWG.

Trade services and technical Assistance

Paragraph 6.1.2 of the JCPOA text covers the provision of services and assistance in conducting nuclear-related trade with Iran. The measures in this paragraph apply to both dual-use and Trigger List goods. The inclusion of dual-use goods in the scope of this paragraph is unusual and will create substantial challenges for the trade service sectors, including the shipping, finance and insurance sectors. In this context, UN Security Council document S/2015/28 provides a starting point in considering how commercial entities might comply.[6]

Arms

From implementation day, the export of arms to or from Iran will no longer be prohibited as they were under the terms of UN Security Council resolution 1929. Instead, exports of arms to Iran would require the authorisation of the UN Security Council (an authorisation that may not be forthcoming as any of the permanent members of the Security Council could use its veto to prevent such transfers). These measures will stay in place for a period of five years.

Missiles and related technology

Resolution 2231 'calls upon' Iran to stop pursuit of ballistic missiles and prohibits states from exporting missiles and related technology to Iran, as defined by the Missile Technology Control Regime, for a period of up to eight years unless authorised by the UN Security Council in advance. Again, such authorisation is unlikely to be forthcoming. It should be noted however that Iran's leadership has stated that it will ignore the call to cease development of ballistic missiles and has already announced new ballistic and cruise missile systems. The restrictions on missile technology are therefore likely to be a key point of contention in the years ahead, with Iran likely to continue to try to covertly acquire controlled dual-use items with missile applications from the international marketplace.

The role of the PWG

In addition to the European External Action Service, which will administer the Procurement Working Group, there will be seven participating states: the UK, U.S., France, Germany, Russia, China and Iran.

The PWG will respond to specific requests by states to export goods to Iran. In practice, this will involve each state (see below) forwarding to the PWG licence applications received at the national level that are deemed relevant to the JCPOA. The

participants will have 20 working days (extendable to 30) to consider any one export. The review will take place in parallel to national export licence assessment.

The PWG requires consensus to authorise exports to Iran: if any one participant objects, the export will not be approved. However, any party can refer cases to the PWG's parent body, the Joint Commission, if they feel that the JCPOA is not being honoured (i.e., Iran could take issue with the refusal of a licence and refer it to the Joint Commission).

It is not yet clear if and how often referrals may be refused. Reasons for refusal are likely to include the risks of stockpiling and the risk of diversion to military and missile end uses. If the JCPOA breaks down, the Procurement Channel will cease operation.

The number of cases that the PWG will have to review is difficult to predict. The number of exports to nuclear end uses is likely to be relatively low. However, the inclusion of NSG dual-use goods in the scope of work for the Procurement Channel could greatly expand the number of cases it reviews. The closest parallel is the case of Iraq in the 1990s. The International Atomic Energy Agency's Iraq Nuclear Verification Office purportedly reviewed some 18,000 contracts over its lifetime.

The potentially high volume of referrals creates challenges. Each participating government must be able to review each referral as if it was an export licence. Typically, an individual licence assessor at the national level may deal with a few hundred to (at most) a few thousand licence applications per year. Applied to the PWG, this could mean that each participating government would need to devote several specialist staff to the task. This will be particularly important given the relatively tight timescales for the review of licence proposals (20 working days).

The JCPOA also does not define what language referrals should be submitted in (although the JCPOA does say that the working language of the JCPOA will be English), so there is a possibility that translation time would also need to be accounted for.

The role of the IAEA

The IAEA is requested to monitor and verify the JCPOA. In practice, in the context of the Procurement Channel, it is possible that the IAEA will have to confirm that any procurements made through the Procurement Channel are consistent with the JCPOA, although there is ambiguity in the text of the JCPOA. This will mean ensuring that the end use for nuclear goods has been declared and that the number of goods being procured is consistent with the needs of the programme (i.e., that goods are not being unduly stockpiled). The IAEA will have to act promptly for this role to be carried out successfully: those states that participate in the Procurement Channel are required to indicate within 20 working days whether or not they object to the proposed export.

The second role for the IAEA is likely to be in verifying that goods imported to Iran are being used as intended. This will involve conducting end-use verification of export of Trigger List items to Iran. Therefore, the IAEA would have to be selective about which imports it undertakes end-use verification. In practice, this task will likely be wrapped into the IAEA's inspection plan for Iran which already includes periodic visits to some sites. It is conceivable that visits may be required for other sites, meaning that the access process specified in the JCPOA would be used.

The third role will be in monitoring Iran's declarations against Iran's actual imports. This is routine business for the IAEA, although in the case of Iran the IAEA will have access to additional information provided by Member States.

The role of the UN and Security Council

The adoption of Resolution 2231 makes clear that the UN Security Council will have a direct role in implementing aspects of the JCPOA. Perhaps the primary defined role of the UN Security Council is in considering or noting exports to Iran of arms, missile technologies and light water reactor technologies. As mentioned, the UN Security Council must review, and then permit or deny, proposed exports of arms and missile-related technology on a case-by-case basis for a period of five years and eight years, respectively. The Security Council will also take note of exports of light water technology to Iran. In none of these cases will the case first be referred to the PWG – instead, states will submit such cases

Necessary information

(a) a description of the item; (b) the name, address, telephone number, and email address of the exporting entity; (c) the name, address, telephone number, and email address of the importing entity; (d) a statement of the proposed end use and end-use location, along with an end-use certification signed by the AEOI or the appropriate authority of Iran attesting the stated end use; (e) export licence number if available; (f) contract date, if available; and (g) details on transportation, if available; provided that if any of the export licence number, contract date, or details on transportation are not available as of the time of submittal of the proposal, such information will be provided as soon as possible and in any event as condition of approval prior to shipment of the item.

directly to the Security Council through a mechanism that is yet to be specified.

The second likely role for the UN (and possibly more specifically the UN Security Council) is investigating specific cases of non-compliance and assisting states to implement the resolution and JCPOA. There is still uncertainty around this role, however, as resolution 2231 acts to disband the Panel of Experts established pursuant to sanctions resolution 1929, which previously fulfilled this role.

The Role of industry and the private sector

The Procurement Channel exists to facilitate trade. Industry and the private sector can benefit from the existence of the Procurement Channel. Nonetheless, it is not envisioned that there will be direct interaction between the Procurement Channel and industry in terms of referrals. Instead, national licensing agencies will act as go-betweens, referring cases to the Procurement Channel as necessary.

The only foreseen exception to this rule is with regards to awareness-raising and outreach. Procurement Channel officials might, with the consent of national authorities, conduct awareness-raising activities for the private sector. This could include issuing guidance on compliance and due diligence. The Joint Commission should provide assistance and guidance to states to undertake such outreach.

It should be noted that paragraph 6.1.2 appears to require trade service providers to take measures beyond those that they usually would for traditional export controls. Further guidance on interpreting this paragraph will be required.

The Role of Iran

Iran's central role in the Procurement Channel has some interesting elements. Iran will participate in the Procurement Working Group and be involved in the decision-making process to decide what goods it can and cannot import, although Iran cannot override decisions of the other members on its own. Iran is also required to attest that the stated end use for goods that it imports through the channel is accurate. Specifically, Iran is required to provide 'a statement of the proposed end use and end-use location, along with an end-use certification signed by the Atomic Energy Organisation of Iran or the appropriate authority attesting the stated end use'.

This latter role is unusual: usually, it is the actual end-user that would sign an end-user undertaking. By requiring bodies authorised by the Iranian government to sign end-user undertakings, the Joint Commission can hold the Iranian government responsible for diversion of any products. It does, nonetheless, require Iran to put in place mechanisms to provide such attestation. It is also unusual for commercial entities that are importing goods to be required to know the control status of the goods. Therefore, an industry outreach and education campaign will be required in Iran.

The Role of Other states

The purpose of the Procurement Working Group is to consider exports of nuclear-relevant goods from other states to Iran. Conceivably, Iran could import such goods from any of the 193 UN member states (and indeed other countries). Therefore, a central aspect of the Procurement Channel will involve referral of relevant exports from states to the Procurement Channel. This will most likely be implemented by export-licensing organisations in each state. Logistics and practical matters will have to be worked out, including in relation to the language of submission.

States will also be able to (and in some cases required to) conduct end-user verification of dual-use exports to Iran. The Joint Committee will provide assistance to states in undertaking this activity and Iran is required to provide access to conduct such end-use verification. Nonetheless, this could be a resource-intensive task for states and may deter some states from exporting goods to Iran when end-use verification would be necessary.

Monitoring illicit procurement

Iran's nuclear programme has been constructed largely using goods that have been imported illicitly from other countries. The JCPOA includes a requirement that all procurement be made through the Procurement Channel specifically to prevent illicit trade in the future.

A continuance of illicit trade would thus constitute non-compliance with the agreement. The Security Council resolution supporting the JCPOA spells out the consequences of such non-compliance, but if taken to its fullest extent, a violation could result in the use of the UN sanctions snapback mechanism.

Details of how possible violations will be investigated have not yet been announced. It is understood that the Panel of Experts established to monitor implementation of UN sanctions (established pursuant to resolution 1929) will be disbanded. This potentially leaves a substantial gap as, in addition to investigating non-compliance, the panel also assisted states with implementation of the sanctions resolutions.

Broader issues

The Procurement Channel is a hugely complex mechanism. As such, it raises numerous broader issues and challenges.

Commercial confidentiality

In order to be able to review referrals, the PWG will require access to key information on proposed exports (see box 'Necessary information'). The need to share commercial information with several states could naturally cause concerns about confidentiality at the national or industry level. It is notable, therefore, that the provision of certain information (including pricing information) is not specifically required under the JCPOA terms. Nonetheless, exporters may be hesitant about providing other required information and assessors may be

Links and notes

[1] For the complete text of the JCPOA, see 'Iran deal – an historic day', EEAS Website: http://eeas.europa.eu/top_stories/2015/150714_iran_nuclear_deal_en.htm (Accessed 16/07/2015)

[2] The closest precedence is the mechanism implemented against Iraq in the 1990s.

[3] See 'Parameters for a Joint Comprehensive Plan of Action Regarding the Islamic Republic of Iran's Nuclear Program', U.S. Department of State, 2 April 2015. Available online at: http://www.state.gov/r/pa/prs/ps/2015/04/240170.htm (Accessed 16/07/2015)

[4] Paragraph 6.1.3 also addresses the issue of whether Iran can buy stakes in uranium producing entities outside the territory.

[5] The Security Council resolution may contain exclusions for light water reactors, which are exempt from the current sanctions resolutions.

[6] S/2015/28: 'Sanctions compliance in the maritime transport sector', .15 January 2015. Available online at: http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/28 (Accessed 16/07/2015)

[7] Actually, an outdated version of the Trigger List from the 1990s.

hindered by the lack of pricing information. This trade-off has nonetheless been agreed.

Corruption

The requirement for the Iranian government or authorised parties to provide attestation for end-use undertakings could lend itself to corruption and profiteering. The Joint Commission may thus wish to monitor who in Iran is involved in the authorisation (i.e. whether they have links with the Islamic Revolutionary Guards Corps or other entities about whom the international community retains concerns).

Precedence for other states

The JCPOA makes clear that it does not set a precedent for other states. Nonetheless, consideration should be given in due course as to what the implications of the Procurement Channel are for the international non-proliferation framework. Presently, states that implement an additional protocol to their safeguards agreement with the IAEA provide the IAEA with reports on exports (and imports) of certain Trigger List goods.[7] Could and should this reporting requirement be extended to dual-use goods? Are there grounds for extending the requirement for the IAEA to verify the nuclear need associated with Trigger List transfers? These are questions that are politically difficult. Nonetheless, they should be considered in the fullness of time.

Conclusions

The Procurement Channel will be perhaps the most complex aspect of the JCPOA to implement. It requires all states to implement complex measures and requires Iranian persons and entities to cooperate. Nonetheless, the modalities outlined in the JCPOA do appear to be implementable, although several practical issues must still be addressed. Before implementation day, further work is required in order to fully set out what is required for each of the parties involved in implementation.

Ian J. Stewart, Head Project Alpha, King's College London.
www.acsss.info
ian.stewart@kcl.ac.uk

Striking a balance between investment liberalisation and national security in China-U.S. relations




The Chinese and U.S. markets present opportunities for each country. Tatman R. Savio, Stephen S. Kho, Cynthia Y. Liu, and Lucy (Qiong) Lu discuss the ongoing bilateral investment treaty ('BIT') negotiations against the backdrop of national security concerns.

For decades, foreign direct investment ('FDI') between the United States and China was characterised by American multinational companies investing in labour-intensive manufacturing and consumer-oriented operations in China.[1] In the past several years, however, China's FDI in the U.S. market has increased dramatically, moving beyond significant purchases of Treasury bonds and other securities by sovereign investors to investments by Chinese companies in a myriad of advanced technologies, brands, and real estate in the United States.[2] The Chinese and U.S. markets present a wealth of opportunities for each other, and current and upcoming regulatory and political priorities in both countries will shape the trajectory and dynamics of their economic relationship well into the future. This article explores the potential for continued economic liberalisation between the two countries with the ongoing bilateral investment treaty ('BIT') negotiations, against the backdrop of national security concerns and related developments that may threaten to undermine a more expansive economic future.

Current and proposed restrictions on foreign investment

Based on traditionally accepted principles of international law, countries have the sovereign power to exclude foreign persons and property, and to prescribe the terms and conditions on which foreigners may enter their territory.[3] Notwithstanding these powers of exclusion, most countries are able to participate in cross-border trade and investment through various international trade agreements and BITs. However, even under these agreements, countries maintain the right to regulate foreign investments and trade in order to protect their national security interests.[4] As a result, despite trends towards greater economic and investment liberalisation, many countries, including the United States and China, maintain laws that proscribe foreign investment in particular sectors and require government review and prior approval of certain other foreign investments.

The U.S. foreign investment review process

Under the Exon-Florio amendment to the Defense Production Act (the 'Exon-Florio law'), the inter-agency Committee on Foreign Investment in the United States ('CFIUS') has the authority to conduct national security reviews and investigations of transactions that could result in foreign control of a U.S. business.[5] The Exon-Florio law authorises the President to block such a transaction (or order divestment of a completed transaction) if there is credible evidence that foreign control of the U.S. entity 'threatens to impair' U.S. national security, and existing legal provisions do not provide adequate protection. Although

notifying CFIUS of a proposed foreign investment transaction remains voluntary, many parties proactively seek CFIUS clearance to eliminate potential future liability under the Exon-Florio law.

In 2007, the U.S. government enacted the Foreign Investment and National Security Act ('FINSA') in response to U.S. public and political criticism of several high-profile transactions that raised concerns about the sufficiency and effectiveness of CFIUS to protect U.S. national security. Among other changes, FINSA expanded the scope of national security reviews, created a presumption for investigations of certain transactions (e.g., those involving critical infrastructure), and increased Congressional oversight of proceedings. It also required the consideration of additional factors in assessing the national security implications of a proposed transaction, and increased the number of agencies involved in CFIUS reviews and investigations.

In the years following FINSA's enactment, Chinese investors voiced concerns that the U.S. government unfairly targeted Chinese companies in the CFIUS process. Notwithstanding these concerns, Chinese investors have actively engaged the U.S. market in recent years, with China accounting for the most CFIUS notices filed (21) by a foreign country in FY2013, and representing 22% of the total notices reviewed in that period.[6] Of course, the data does not capture the full complexity or nuances of Chinese investment in the U.S. market, including investors who back off from U.S. deals, restructure them to mitigate Chinese majority ownership or control, or abandon transactions all together, as a result of actual or perceived pressure from the CFIUS process.

China's foreign investment review process and national security initiatives

Current process

China regulates foreign investment through various mechanisms under disparate legal regimes. For foreign investment purposes, China characterises industries as 'encouraged', 'restricted', or 'prohibited' under the *Foreign Investment Guidance Catalogue*.[7] Any industry not listed in this catalogue falls under the 'permitted' category. Except for such activity in China's four free trade zones ('FTZs') (Shanghai, Guangdong, Tianjin, and Fujian – the latter three were established earlier this year), the Chinese government approves foreign investment on a case-by-case basis in what is often a time-consuming process, regardless of which industry category is involved. Moreover, since March 2011, China has subjected foreign acquisitions in specified industries (e.g., defence, agriculture, natural resources, infrastructure, transportation) to a separate national security review process pursuant to a State Council circular,[8] and implementing rules issued by the Ministry of Commerce ('MOFCOM') ('2011 NSR Rules').[9]

Proposed national foreign investment law and negative list

On 19 January 2015, MOFCOM issued the draft Foreign Investment Law ('FIL'), which promises to streamline the existing Chinese foreign investment regime by replacing various laws currently in place (e.g., the Wholly Foreign-Owned Enterprise Law, Sino-Foreign Equity Joint Venture Enterprise Law, and the Sino-Foreign Cooperative Joint Venture Enterprise Law).[10] The FIL significantly alters the structure and process of foreign investment review in China, including by adopting a 'negative list' approach to foreign investment, which is currently employed in all four FTZs in China. Under the proposed approach, foreign investments falling outside the negative list will no longer require approval, although the establishment of a foreign investment enterprise ('FIE') in an industry outside the negative list will remain subject to certain registration requirements and industry-specific licensing regimes as a domestic Chinese company.

For foreign investment in sectors on the negative list or exceeding the prescribed investment amount thresholds (which have not yet been clarified in the FIL), foreign investors will still be required to obtain a 'market entry permit' from the authority responsible for reviewing the foreign investment. While it is uncertain when or whether the FIL will be promulgated, the Chinese government reportedly passed in late September the *Opinion on Implementing the Negative List for Market Entry*. The opinion states that the State Council will formally implement a negative list for the entire country in 2018, after applying it in select regions in trial versions from 2015-2017.

The FIL also provides the basis for a more extensive national security review for foreign investment. As a counterpoint to the general relaxation of foreign investment restrictions and approval requirements described above, the FIL provides that any foreign investments that 'harm or may harm national security' must undergo a national security review, without limiting the industries involved. Similar to the U.S. regime, the FIL establishes a joint committee and gives it broad discretion to assert jurisdiction over a particular transaction, as well as to make national security decisions that are not subject to judicial or administrative review. Unlike the CFIUS process, the FIL does not explicitly address the confidentiality of the national security review process or exclude greenfield investments or certain other types of transactions from the scope of review. Moreover, while the definition of 'national security' captures some factors of the CFIUS process (e.g., critical infrastructure, sensitive technologies, foreign-government controlled transactions), it also allows

News: Sino-U.S. cybersecurity agreement

Following President Xi's recent visit to the United States, the Chinese and U.S. governments have entered into a cybersecurity agreement, in which they agreed, among other commitments, not to conduct or support cyber-enabled theft of intellectual property. For now, this development appears to have preempted U.S. consideration of sanctions against certain Chinese companies for alleged cyber-attacks against U.S. companies. If imposed in the future, cybersecurity sanctions would likely create additional challenges for Chinese companies seeking to invest in the United States, particularly in the technology sector. Moreover, the issuance of such sanctions could impact China's consideration of several pending national security measures.

for consideration of 'social public interests' and 'public order'.

AmCham China, AmCham Shanghai, and the U.S. Chamber of Commerce have cautiously welcomed components of the FIL, including its grant of national treatment to foreign investments not on the negative list. However, they have expressed concern about the potential breadth of China's national security review powers, emphasising that the review process should not extend to areas beyond national security, such as national interest, social stability, economic security, or industrial security. In addition, AmCham China and other groups have voiced concern regarding the lack of guarantees with respect to confidentiality and the bifurcation of the market entry and national security review processes, which could result in duplication of the national security review process.

Separately, on 8 May 2015, the State Council issued *Tentative Measures for the National Security Review of Foreign Investment in the Free Trade Zones* (the 'FTZ NSR Circular')[11] to apply to foreign investments in all four FTZs. According to the FTZ NSR Circular, a committee comprised of representatives from the National Development Reform Commission ('NDRC'), MOFCOM, and other relevant agencies will also conduct national security reviews of foreign investment in the FTZs. The new regime in the FTZs expands on the current 2011 NSR Rules by requiring a national security review of foreign investments in the following industries: defence, agricultural products, energy and natural resources, infrastructure, transportation services, important culture (newly added), important information technology products and services (newly added), and equipment manufacturing enterprises.

Other national security initiatives

China's recent consideration of a series of national security-related laws, including the National Security Law,[12] the Cybersecurity Law,[13] the Counterterrorism Law,[14] and the Administration of Foreign Non-Governmental Organizations Law ('NGO Law'),[15] has enhanced concerns about proclaimed national security issues impeding foreign investment. The National Security Law, which became effective on 1 July 2015, states that its purpose is to '...defend the people's democratic and political power and the socialist system with Chinese characteristics, protect the fundamental interests of the people, ensure the smooth process of reform and opening up to the outside world and the modernisation of socialism, and achieve the great rejuvenation of the Chinese nation'. The law defines 'national security' broadly as 'ensuring that the country's political authority, sovereignty, national unification, territorial integrity, people's welfare, the sustainable development of the economy and society, and other significant national interests are not subject to danger, internal or external threats, and can be guaranteed continued security'. Of particular concern to many is the law's promotion of 'indigenous innovation', as well as its stated goal of maintaining 'secure and controllable' information networks, infrastructure, and systems, which could be interpreted as renewed efforts to block foreign investment, especially in the information technology sector.

Furthermore, China released a draft Cybersecurity Law on 6 July 2015, which, among other objectives, seeks to 'safeguard cybersecurity and maintain cyberspace sovereignty, national security and the social public interests'. The draft law explicitly allows Chinese authorities to cut Internet access during public security emergencies, and requires government agencies to set up cybersecurity monitoring and alert systems and emergency-response measures. Foreign businesses have expressed concern about the impact of this law, especially in the context of other national security-related laws being considered in China.

In addition, China is considering the draft NGO Law, which would require foreign NGOs to register in China and be sponsored by a government organisation. The draft law's broad definition of 'a foreign NGO' ('social organisations that are non-profit and non-governmental, which are established abroad') could potentially capture the activities of trade associations, overseas chambers of commerce, and professional associations. In June, over 40 U.S. business and professional groups signed a letter to the Chinese government expressing concerns that the law would restrict their activities and damage U.S.-China relations. The European Chamber of Commerce in China also expressed concern regarding the administrative burden of the proposed law and its impact.

In early 2015, due to widespread criticism, the China Banking Regulatory Commission ('CBRC') suspended previously-issued guidance requiring Chinese financial institutions to ensure at least 75% of their information technology infrastructure used 'safe and controllable' products and services by the end of 2019. Many interpreted this provision, in conjunction with other requirements, to mandate the use of Chinese-developed products and services. China has also reportedly pledged to remove discriminatory provisions against

foreign firms from the banking regulations, as part of the commitments made at the 2015 U.S.-China Strategic and Economic Dialogue ('S&ED').[16]

In March 2015, in the face of strong opposition and direct criticism from President Obama, the Chinese government put on hold its draft Counterterrorism Law, which would have required foreign technology firms to provide Chinese authorities with access to computers and information networks, as well as encryption keys and source code, among other requirements.

Potential for the U.S.-China BIT to improve prospects for foreign investment

Against the backdrop of China's FIL and national security initiatives are a number of recent political and economic events, including instability in China's financial markets, the devaluation of the renminbi, the recent cybersecurity agreement between the United States and China, and the even more recent Trans-Pacific Partnership ('TPP') deal. In relation to these events, the ongoing negotiations between China and the United States to establish a BIT provide an avenue for engagement between the two countries, both economically and politically. China and the United States have been engaged in BIT negotiations since 2008. The two countries have experienced significant roadblocks along the way, including the election of President Obama, who until recently had prioritised other initiatives. As China moves forward with the FIL and other national security laws, the BIT can be a tool for assuring U.S. investors that China's recently renewed national security focus will not foreclose foreign investment. The BIT can also be an avenue for the U.S. government to assuage Chinese concerns that it is unfairly targeted in the CFIUS process with respect to investment in the U.S. market.

Overview of the substantive disciplines in the BIT

As a general matter, a BIT is a reciprocal, international agreement regarding how nations should treat foreign investment. A country's model BIT is usually the text that forms the starting point for negotiations. However, the BIT negotiation process is dynamic and unique to each trading partner. As a result, the provisions of any given BIT can vary depending on the parties involved.

The United States negotiates BITs on the basis of a 2012 model text ('U.S. Model BIT'),[17] which focuses on protecting U.S. investments abroad. Up until the 1990s, China's BITs were characterised by limited protections for foreign investors. However, recent Chinese BITs contain many of the standard provisions found in global BIT practice, including the foundational disciplines of non-discriminatory and minimum standard of treatment.

The bilateral investment treaty can be a tool for assuring U.S. investors that China's recently renewed national security focus will not foreclose foreign investment.

The non-discrimination principle is a fundamental component to BITs, providing that the host nation will not discriminate against foreign investment. The standards of non-discriminatory treatment most commonly included in BITs are national treatment and most-favoured-nation ('MFN') treatment. National treatment requires that, in 'like' circumstances, each party treat investors of the other party no less favourably than its own investors. MFN treatment similarly requires that, in 'like' circumstances, each party treats investors of the other party no less favourably than investors from third countries. In addition, BITs usually require that the host nation accord covered foreign investments 'fair and equitable treatment' (e.g., due process protections), as well as 'full protection and security' or equivalent standards (e.g., the level of police protection for foreign investments that is required under customary international law), as the minimum standard of treatment. This minimum standard of treatment is an absolute standard, governing how a host nation must treat foreign investments regardless of how the host nation treats its own nationals or other third-party investments.

In addition, most BITs include provisions on expropriation, free transfers, and investor-state dispute settlement procedures, among other protections. Also relevant to countries' national security interests is the possible inclusion of security and prudential exceptions in the core text of a BIT. Such exceptions allow the parties to apply measures necessary for the protection of its 'essential security interests', as well as measures relating to financial services for 'prudential reasons', such as for the protection of investors, depositors, policy holders, or persons to whom a fiduciary duty is owed by a financial services supplier, or to ensure the integrity and stability of the financial system.

BITs may address market access commitments through the use of a 'negative list' approach or a 'positive list' approach. With a 'negative list' approach, countries specifically carve out sectors for which they will restrict foreign investment. Alternatively, a 'positive list' approach specifies only those sectors for which countries are willing to make investment liberalisation commitments, leaving the remainder closed to foreign investment. In addition, the United States usually favours the 'pre-establishment' model in its BITs, which prevents host countries from discriminating against foreign investment during the stages leading up to the actual investment, such as by imposing an outright quota limiting FDI in covered sectors.

Recent developments in U.S.-China BIT negotiations

While the negotiations are confidential, it is expected that the U.S.-China BIT core text will include many, if not all, of the substantive disciplines discussed above. Moreover, at the July 2013 S&ED, the U.S. government touted as a significant breakthrough commitments made by China that it would negotiate the U.S.-China BIT using a 'negative list' approach, and would commit to protections in all stages of investment pursuant to the 'pre-establishment' model.[18]

While discussions on the core text are ongoing, the United States and China finally exchanged their initial "negative list" offers during the 19th round (June 8-12, 2015) of negotiations. During the most recent 21st negotiating round in early September 2015, the United States and

China exchanged revised negative list offers.[19] Reports in the trade press and reactions from experts familiar with the negotiations have indicated that while China's negative list improved in the most recent negotiating round, it still contains a long list of industries or sectors that will be excluded from China's investment liberalisation commitments.[20] Both countries agreed to 'intensify negotiations' during President Xi's recent U.S. visit, although many experts predict that negotiations may extend beyond 2016.[21]

Balancing security interests with investment liberalisation

China's overall record on encouraging and protecting foreign investments has been mixed. On the one hand, it has shown a willingness to adopt a negative list approach to investment, including with respect to the BIT negotiations with the United States. On the other hand, it has still included a significant number of industries, which are either forbidden or restricted to foreign investors, on the negative list applicable to the FTZs. The Chinese government has not yet released the negative list that will apply under the FIL or the *Opinion on Implementing the Negative List for Market Entry*, nor has it explained how it will align with the negative lists applicable to the FTZs currently in place. Moreover, China may restrict foreign investment through a more extensive national security review process. These factors have resulted in uncertainty and scepticism regarding China's overall commitment to investment liberalisation.

The United States has similarly drawn criticism from China for the opaqueness and politicisation of the CFIUS review process. In 2012 and 2013, more investments from China underwent CFIUS review than from any other country.[22] For China, the number of CFIUS reviews from 2010 to 2013 has nearly quadrupled, which may be interpreted to represent growing acquiescence among Chinese companies that they must submit to the U.S. national security process.[23] China has also complained that the investment climate in the United States has been quite negative for Chinese firms. In this regard, Chinese government officials have cited U.S. investment restrictions in the infrastructure and financial sectors as one of the main barriers for Chinese investors.[24]

For the U.S.-China BIT negotiations to conclude successfully, both the United States and China must seek to strike the right balance between their national security interests and commitments to investment liberalisation. First, both countries should present strong negative list offers and limit the sectors that are carved out from the BIT disciplines to only those that are considered critical infrastructure, or truly implicate national security interests (e.g., defence, emergency services). In addition, economic interests should not be conflated with security interests, and any security or prudential-related exceptions should be narrowly crafted.

Overall, the BIT offers an opportunity at the highest levels for U.S. and Chinese officials to chart the economic relationship of the two countries for the future. Ongoing dialogue will be especially important as the United States moves forward with finalising the historic TPP trade deal, which includes many countries in Asia, but not China. For the United States, increased Chinese investment will translate, in many cases, into economic growth and job promotion. In China, increased U.S. investment will lead to the development of higher value-added products and services and technical expertise. To achieve their economic goals, both countries must be willing to make commitments to ensure an open, transparent and predictable investment environment. While market access should not translate into an abdication of national security interest, both countries should view circumspectly the efforts of the other to invoke these grounds to foreclose investment, and focus instead on ways to move their relationship forward for reciprocal benefits.

Tatman Savio and Stephen Kho are partners, Cynthia Liu is an associate, and Lucy (Qiong) Lu a counsel at international law firm Akin Gump.

tatman.savio@akingump.com

lskho@akingump.com

liuc@akingump.com

lucy.lu@akingump.com

Links and notes

1 Daniel H. Rosen and Thilo Hanemann, New Realities in the US-China Investment Relations, Rhodium Group-US Chamber of Commerce (April 2014), available at https://www.uschamber.com/sites/default/files/documents/files/RHG_New%20Realities_29April2014.pdf.

2 Id.

3 Michael V. Seitzinger, Foreign Investment in the United States: Major Federal Statutory Restrictions, Cong. Research Serv., June 17, 2013, available at https://www.fas.org/sgp/crs/misc/RL33103.pdf.

4 See, e.g., General Agreement on Tariffs and Trade (GATT), Art. XXI; General Agreement on Trade in Services (GATS), Art. XIVbis; 2012 U.S. Model Bilateral Investment Treaty, Art. 18.

5 50 U.S.C. App. 2170 (d)(1).

6 CFIUS, Annual Report to Congress CY 2013, issued Feb. 2015, http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2014%20CFIUS%20Annual%20Report%20for%20Public%20Release.pdf

7 For a copy of the most updated Foreign Investment Guidance Catalogue issued in March 2015, see http://www.sdpc.gov.cn/zcfb/zcfbl/201503/W020150402620481787669.pdf.

8 State Council, Circular on the Establishment of a Security Review Process for Mergers and Acquisitions of Domestic Enterprises by Foreign Investors, March 2011, available at http://www.gov.cn/zwgk/2011-02/12/content_1802467.htm.

9 Ministry of Commerce (MOFCOM), Implementing Rules Regarding the Security Review Process for Mergers and Acquisitions of Domestic Enterprises by Foreign Investors, Sept. 2011, available at http://www.mofcom.gov.cn/aarticle/b/c/201108/20110807713530.html.

10 For a copy of the Chinese language version of the draft FIL issued on January 19, 2015, see http://www.mofcom.gov.cn/article/ae/ag/201501/20150100871007.shtml.

11 State Council, Tentative Measures for the National Security Review of Foreign Investment in the Free Trade Zones, May 2015, available at http://www.china-shftz.gov.cn/PublicInformation.aspx?GID=26c11407-27be-4ee2-88de-2976aff0e251&CID=953a259a-1544-4d72-be6a-264677089690&MenuType=1.

12 National Security Law, available at http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm

13 Cybersecurity Law (reading draft), available at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

14 Counterterrorism Law (Second Reading Draft), available at: http://www.npc.gov.cn/npc/xinwen/2015-02/27/content_1906005.htm.

15 Administration of Foreign Non-Governmental Organizations (Second Reading Draft), available at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-05/05/content_1935666.htm.

16 2015 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet – Economic Track, June 25, 2015, available at http://www.treasury.gov/press-center/press-releases/Pages/jl0094.aspx; U.S., China Agree to Exchange New BIT Negative Lists by September, Inside U.S. Trade, June 25, 2015.

17 The 2012 U.S. model BIT is available at: http://www.state.gov/documents/organization/188371.pdf.

18 See Press Release, U.S. Dep't of Treasury, U.S. and China Breakthrough Announcement on the Bilateral Investment Treaty Negotiations, 15 July 2013: http://www.treasury.gov/connect/blog/Pages/U.S.-and-China-Breakthrough-Announcement-.aspx.

19 U.S., China Exchange Improved 'Negative-List' Offers at 21st BIT Round, *Inside U.S. Trade*, 17 September 2015.

20 Froman Says China's Latest BIT Offer Insufficient; Seeks Progress at Xi Visit, *Inside U.S. Trade*, 24 September 2015

21 China Agrees Not to Engage in Cybertheft of Trade Secrets, Following Xi Visit, *Inside U.S. Trade*, 1 October, 2015..

22 CFIUS, Annual Report to Congress CY 2012, issued Dec. 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2013%20CFIUS%20Annual%20Report%20PUBLIC.pdf. See also CFIUS, Annual Report to Congress CY 2013, issued Feb. 2015, http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2014%20CFIUS%20Annual%20Report%20for%20Public%20Release.pdf.

23 Id.

24 U.S., China Agree to Exchange New BIT Negative Lists by September, *Inside U.S. Trade*, 25 June 2015.

EU/Iran: Aviation

Dealing in the aviation sector until the expected extensive relief of sanctions


European commercial aviation companies attracted by possible new business opportunities in Iran must not forget the current EU and U.S. sanctions regimes in their rush for business, write Brian Mulier and Goran Danilovic.

On 14 July 2015 the Joint Comprehensive Plan of Action ('JCPOA') was signed by the E3/EU+3 countries and Iran. The United Nations Security Council endorsed the JCPOA by enacting UN Resolution 2231 (2015). The JCPOA comprises a monitoring system, timetable and steps to be taken by Iran with regard to its nuclear programme as well as the commitments of the United States and European Union to provide relief of their current sanctions regimes against Iran.

JCPOA implementation

The JCPOA provides for a phased implementation of the agreement as shown below. Taking into account that the implementation process is prone to political sentiment, certain dates provided in the below matrix should be considered as estimates.

In addition, it is noted that EU sanctions lifted following Implementation Day of the JCPOA agreement can be reversed. UN Resolution 2231 (2015) and JCPOA provide for a so-called 'snap back' option which, when evoked, would reinstate the EU sanctions regime. If reinstated, the EU sanctions would not apply with retroactive effect to contracts signed between any party and Iran or Iranian individuals and entities prior to the date of its application, taking into account that these activities are consistent with the JCPOA and UN Resolution 2231 (2015) and previous UN resolutions. The 'snap back' liability should be taken into account when doing business in Iran, e.g. by including anticipatory contractual provisions.

Commercial aviation

Can EU companies engage in the commercial aviation sector in Iran prior to the extensive relief of the sanctions under the JCPOA?

As illustrated below, the main EU commitments as set forth in the JCPOA have not been implemented by the EU yet. This means that, at this stage, Iran is still subject to an extensive EU sanction regime regime prohibiting a vast amount of activities, including those related to the aviation sector. Upon reaching agreement on the JCPOA, the EU did prolong the existing EU temporary sanction relief that will continue to be in force until 14 January 2016. In that regard, the EU temporary

JCPOA implementation (EU perspective)

Phases	Date/expected	Effects for EU business
Finalisation Day	14 July 2015	NO, considering that the current EU sanctions regime remains in place.*
Adoption Day	(est.) 18 October 2015 (or earlier if agreed by E3/EU+3 and Iran)	NO, the current EU Sanctions regime remains in place. EU will enact an EU regulation, terminating and suspending all nuclear-related economic and financial EU sanctions, taking effect on Implementation Day.
Implementation Day	Expected 6 months after Adoption Day (est.) early/mid 2016	YES, large parts of nuclear-related economic and financial EU sanctions will be terminated and suspended. Numerous UN Security Council resolutions will be terminated subject to re-imposition in the event of significant non-performance by Iran of JCPOA commitments. Specific restrictions, including restrictions regarding the transfer of proliferation sensitive goods will apply.
Transition Day	(est.) October 2023 (or earlier based on IAEA report and supporting UN Security Council)	YES, further relief of EU sanctions regime by terminating and suspending certain EU sanctions provisions still in place.
Termination Day	(est.) October 2025	YES, EU will terminate all remaining EU sanctions.

** Following the signing of the JCPOA agreement and the subsequently adopted UN Resolution 2231 (2015) endorsing the deal, the EU has enacted Regulations (EU) 2015/1327 and 2015/1328 amending and supplementing certain aspects of the EU sanctions regime in order to allow for Iran to meet its first obligations under the JCPOA as regards its nuclear programme.*

Exploratory activities by EU companies in Iran	Possible under EU sanction regime?
Travel to Iran	YES
Engage in transactions incidental to such travel	YES
Initiating brokering services or negotiating a contract or transaction aimed at leasing or selling an aircraft	NO
Hold a general presentation marketing expertise and experience of the company	YES - refrain from sharing in-depth knowledge / do's and don'ts.
Hold a presentation covering general topics such as: ● transfer of title/ownership ● mortgage ● registration requirements ● sale, leasing and financing transactions ● title insurance ● bank financing ● escrow agents (management, etc.)	YES provided that the information is not made available to or for the benefit of a currently sanctioned listed entity, body or individual in Iran. TIP: start your presentation with a general remark that you will refrain from commenting on any questions on actual real-life transaction attendees may ask you including in-depth discussion or sharing of knowledge.
Discussing and sharing of technical information and/or providing technical assistance in the form of technical support related to: ● repairs ● development ● manufacture ● assembly ● testing ● maintenance ● instruction ● advice ● training ● transmission of working knowledge ● skills ● consulting services	NO, if it relates to technical information and assistance regarding military or dual-use items or items listed in the EU sanction regime. If it does not concern a military or dual-use item or item listed in the EU sanction regime, refrain from making the information available to or for the benefit of a currently sanctioned listed entity, body or individual in Iran. TIP: check whether the technical information contains US content and, if so, consult U.S. Iran sanction regime provisions. Do also bear in mind that services activities are very broadly defined under the US Iran sanction regime.
Discussing potential sale of goods (e.g. aircraft parts) to be used in the commercial aviation sector	YES, to the extent it does not concern the sale of a military or dual-use item or an item listed in the EU sanction regime or the sale to a listed person. TIP: check whether the item to be sold contains US content and, if so, consult U.S. Iran sanction regime provisions. Do also bear in mind that services activities are very broadly defined under the U.S. Iran sanction regime.
Discussing potential supply of services to be provided to the commercial aviation sector	YES, to the extent the services do not relate to a military or dual-use item or an item listed in the EU sanction regime or will be supplied to a listed person. TIP: Bear in mind the interplay with U.S. Iran sanction regime if the supply of services includes involvement of a U.S. person or the supply of items with U.S. content.
Hire local council in Iran	YES, to the extent the envisaged activities for which council is requested do not fall foul to the EU sanction regime.
Transfer of funds involving EU persons, entities or bodies, including EU financial and credit institutions, and Iranian persons, entities or bodies, including Iranian financial and credit institutions	YES, to the extent that the transfer of funds is not connected to an activity prohibited under the EU sanction regime. If the transfer of funds relates to an activity not prohibited under the EU sanction regime, subsequent notification and authorization requirements exist depending on amount concerned. TIP: Although the EU sanction regime provides for the formal possibility of transferring funds, practice has shown that EU financial and credit institutions will not process transfers of funds in relation to Iran as to avoid any exposure.
Provide or brokering insurance or re-insurance to an individual	NO. If an individual is acting in private capacity and is not one of the listed persons by the EU sanction regime, insurance or re-insurance, including health and travel insurance, is authorized.
Provide or brokering insurance or re-insurance to non-Iranian legal persons, entities or bodies for activities conducted in Iran	NO. If the activities in Iran comprise loading, unloading or safe transit of an aircraft temporarily in Iranian airspace, insurance or re-insurance is authorised.

EU/Iran: Aviation

sanction relief (encompassing relief on certain provisions dealing with petrochemicals, shipping and insurance and funds transfer controls) remains the main playground drawing for doing business with Iran.

Following comments set forth in the above matrix, it can be derived that undertaking any (exploratory) activities in the aviation sector in Iran until the expected lifting of the EU sanction regime by Implementation Day in 2016 is to be handled cautiously. The foregoing means that any (exploratory) activities must be compliant with the (still) existing extensive EU sanction regime, including the earlier mentioned EU temporary sanction relief. Such compliance is to be fully substantiated by the underlying facts and circumstances of activity concerned or, in case of non-compliance, demonstrate that there was no knowledge or reasonable cause to suspect that such (exploratory) activity would infringe any of the provisions of the current EU sanction regime against Iran.

In short, exploring any activities in the aviation sector related to Iran must be weighed against the current EU Iran sanction regime (and possibly U.S. Iran sanction regime) and undertaken in compliance therewith – see the table on the previous page.

Furthermore, bear in mind that the U.S. sanction regime against Iran may also be applicable where your company is regarded as a U.S. person or the underlying (exploratory) activity has content of U.S. origin or involves an activity falling under the scope of the U.S. Iran sanction regime. We note that the U.S. has set in place a favourable licensing policy regime through which specific authorisation can be obtained in order to engage in transactions to ensure the safe operation of Iranian commercial passenger aircraft, including transactions involving Iran Air, but excluding all other sanctioned and listed Iranian airlines.

Undertaking any (exploratory) activities in the aviation sector in Iran until the expected lifting of the EU sanction regime by Implementation Day in 2016 is to be handled cautiously.

In conclusion, Iran remains a challenging place to do business as any preliminary (re-)engagement in the aviation sector in Iran is still subject to the current EU sanction regime against Iran until the expected relief in 2016. Notably, the EU sanction regime is and will be enforced by competent authorities in the EU. This means that compliance should remain on top of the agendas of businesses whilst contemplating and/or conducting any preliminary (exploratory) activities in the aviation sector in Iran.

Brian Mulier is a partner and Goran Danilovic a senior associate in the Hague office of international law firm Bird & Bird.

brian.mulier@twobirds.com

goran.danilovic@twobirds.com

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Ryan Lynch Cathie
www.securustrade.com

Michael Bell
mjvbell@inweb.co.uk

Ian J. Stewart, Project Alpha, King's College, London
www.acsss.info

Tatman Savio, Stephen Kho, Cynthia Liu and Lucy (Qiong) Lu, Akin Gump
www.akingump.com

Brian Mulier and Goran Danilovic, Bird & Bird
www.twobirds.com

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

Researcher, Cristina Rotaru: cristina.rotaru@worldecr.com

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0044]

Correspondence address: D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road,
London N1 7GU, England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road, London, UK

ISSUE 44. OCTOBER 2015
www.WorldECR.com