US: ‘toughest ever’ North Korea sanctions

WorldECR visits the James Martin Center for Nonproliferation Studies in Monterey

Demystifying delisting: A guide to seeking removal from international sanctions lists

OFAC’s pivot to Asia: new risks emerge

CSE and the long arm of US sanctions

Peru: Dual-use export controls in transit and transhipment

The missile sanctions gap: realigning US and EU Iran designations

Smart contracts, blockchain and export control compliance
‘Toughest ever’ North Korea sanctions

The US government announced the ‘toughest ever’ sanctions package against North Korea on 23 February, in a move which the US Treasury describes as ‘aimed at disrupting North Korean shipping and trading companies and vessels to further isolate the regime and advance the U.S. maximum pressure campaign.’

Newly designated parties include ‘one individual, 27 entities, and 28 vessels located, registered, or flagged in North Korea, China, Singapore, Taiwan, Hong Kong, Marshall Islands, Tanzania, Panama, and Comoros,’ said the Treasury Department’s Office of Foreign Assets Control (OFAC).

OFAC also issued an advisory which includes details of the ‘deceptive shipping practices’ undertaken by North Korea to evade sanctions, including:

- Physically altering vessel identification
- Ship-to-ship transfers at sea to conceal the origin or destination of cargo
- Falsifying cargo and vessel documents
- Disabling and manipulating collision avoidance systems, including AIS (automatic identification systems)

The advisory includes an overview of sanctions related to the maritime industry, and a list of North Korean vessels ‘capable of engaging in ship to ship transfers of petroleum’.

The sanctions are consistent with and mandated by the Countering America’s Adversaries Through Sanctions Act (‘CAATSA’). In a client briefing, Michael Gershberg of the law firm Fried Frank noted: ‘This round of sanctions will have little effect on U.S. companies, which are already subject to a comprehensive embargo against North Korea. However, these designations provide a basis for potential secondary sanctions against third-country entities, including foreign financial institutions, that conduct or facilitate certain transactions with sanctioned persons.’

Treasury Secretary Steven Mnuchin said: ‘Treasury is aggressively targeting all illicit avenues used by North Korea to evade sanctions, including taking decisive action to block the vessels, shipping companies, and entities across the globe that work on North Korea’s behalf. This will significantly hinder the Kim regime’s capacity to conduct evasive maritime activities that facilitate illicit coal and fuel transports and erode its abilities to ship goods through international waters.’

For further information, see: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180223.aspx

UK under scrutiny for exporting surveillance kit to the Philippines

Labour MP and member of the select committee on arms export controls, Lloyd Russell-Moyle has criticised the UK government for exporting surveillance equipment to the Philippines.

Since his inauguration in May 2016, Philippines’ president Rodrigo Duterte has waged a violent war on drugs, alleged to have resulted in the deaths of thousands of people. Figures from Campaign Against the Arms Trade (‘CAAT’) show that since then the UK has granted arms export licences to the Philippines worth approximately £14m, for items including information security equipment, imaging cameras and information security software.

‘My office has found that the UK licensed ‘spyware’ to the government of President Duterte weeks after he was inaugurated and vowed publicly to kill all the drug addicts in the Philippines,’ Russell-Moyle tweeted. ‘Another case of Tories ignoring human rights provisions in UK arms export law.’

The UK government considers arms licence applications on a case-by-case basis against the Consolidated EU and National Arms Export Licensing Criteria, one of which is whether there is a ‘clear risk’ that the items might be ‘used for internal repression’ or ‘in the commission of a serious violation of international humanitarian law’. In February, the International Criminal Court in The Hague launched an initial inquiry into allegations of crimes against humanity by Duterte.

Concerns about the export of so-called ‘spyware’ are at the heart of a proposed ‘recast’ of the EU dual-use export control regime – which would see the introduction of a ‘human security’ criterion – and a tightening of the control of exports of technology that could be used for surveillance purposes.

Russell-Moyle’s criticism comes at a time when there is unease in the EU over the uneven application of arms export control policy across the bloc. In September 2017, members of the European Parliament voted to tighten EU arms export control, calling for a crackdown on Member States which violate EU arms export control policy.

Edin Omanovic, export control expert at Privacy International, commented: ‘It’s important to bear in mind that the use of this surveillance technology is considered so sensitive that no government agency will admit that they even exist. Yet the UK government has been signing off on hundreds of licences for their export around the world, including to authoritarian regimes which lack basic rule of law and where state surveillance is known to be targeted at activists, journalists, and the opposition.’

‘It is yet another glaring example of why the system is not fit for purpose. The UK government should urgently review all the licences and revoke them if there is no legal framework in place for their use, and bring forward new rules in the UK and at the EU to ensure human rights risks are appropriately considered.’
US curbs defence trade with South Sudan

The US Department of State has issued a final rule adding South Sudan to §126 of the International Traffic in Arms Regulations (ITAR). This means that South Sudan is now included in the list of countries to which prohibited exports, imports and sales to and from certain countries apply. A policy of denial on the export of defence articles and services is now in place, unless the export falls under one of the listed exceptions, which are decided on a case-by-case basis.

The restrictions are in response to the continuing violence by both government and armed opposition in South Sudan, despite a peace agreement brokered in December 2017, which has created a massive humanitarian crisis. The US has stated that it encourages other countries to follow its lead by imposing arms restrictions and is seeking support for a UN Security Council embargo on ‘all arms flows into South Sudan’.

The inclusion of South Sudan is largely symbolic, and will have no practical impact,’ said Doug Jacobson from Washington DC-based Jacobson Burton Kelley. ‘Last year no sales of defence articles were approved to South Sudan.’

Earlier this month the EU Council imposed unilateral sanctions over South Sudan in response to the escalating crisis; the first time it has done so in addition to UN sanctions.

The International Crisis Group has described the need to address the South Sudan situation as one of the African Union’s ‘seven priorities’, commenting: ‘South Sudan’s failed Christmas cessation of hostilities was a stark reminder of how intractable the country’s conflicts remain. Although fighting has diminished from its height in early 2014, violence remains pervasive. Government forces have the military upper hand, but though fewer regions suffer active combat, much of the country still exists in a state between war and peace: poverty, violence and displacement are constant challenges.’

New reform bill would ‘help US maintain its edge’

On 15 February, Ed Royce, Chairman of the United States House Committee on Foreign Affairs, introduced bipartisan legislation which he believes will modernise US export controls on dual-use items and help the United States ensure its ‘technological advantage’.

If made law, Royce said, the Export Control Reform Act of 2018 (H-R 5040) would represent ‘the first real push to establish permanent export controls since the Cold War-era Export Administration Act of 1979 (EAA) lapsed in 2001.’

Amongst key elements of the proposed legislation:

- **Section 106: control lists** Section 106 requires that the president establish a regular interagency review of each list of controlled items. In accordance with such review, the secretary of commerce is required to regularly update such lists to ensure that new items are appropriately controlled, with such controls adjusted as conditions change. Each list of controlled items shall be published in a form that facilitates compliance with it, particularly by small and medium-sized businesses, and academic institutions.

- **Section 107: licensing** This section requires the president to establish a procedure by which the Department of Commerce shall issue licences or other authorisation for the export, reexport, or transfer of items controlled under this title. It also states that no fee may be charged in connection with licence applications for controlled items.

- **Section 108: compliance assistance** This section authorises the president to establish procedures to encourage closer collaboration between the public and private sectors in identifying proliferation or other export control risks to US national security.

- **Section 109: requirement to identify and control critical technologies in export control regulations** This section requires the president to establish an interagency process to identify emerging technologies that are
not identified in any US or multilateral control list, but nonetheless could be essential to US national defence, intelligence, or other areas of national security.

The Act also provides ‘broad authority to the president to enforce US export controls established under this title. Such measures should include the publication of best practices guidelines to assist industry in compliance with US export controls. This section also includes provisions for protection of confidentiality of information relating to licence applications, with exceptions relating to transmission of such information to the Congress and General Accountability Office.’

In introducing the legislation, Royce said: ‘In recent years, the government in Beijing has increasingly forced US companies to hand over sensitive technology as a cost of doing business in China. These types of aggressive policies are undermining our national security and our economy. The Export Control Reform Act of 2018 will modernise our regulatory control system and make clear the US will not tolerate this behavior. It will help our manufacturers and innovators maintain their competitive edge. And it will promote a transparent, multilateral process to keep sensitive technology out of the hands of countries that would use our technology against us.’

For further information, see: https://foreignaffairs.house.gov/press-release/royce-introduces-bipartisan-export-control-reform-bill/

PEOPLE MOVES

Christensen forms new firm
Larry Christensen has left Miller & Chevalier in DC to form The Law Offices of Larry E. Christensen. Christensen, who has a background in private practice, in-house and government, worked in the US Department of Commerce for 11 years in the Office of Chief Counsel of Export Control Administration and as Director of the Regulatory Policy Division. His new practice will focus on the most challenging areas of export control, such as the outer limits of US reexport rules, commodity jurisdiction, encryption and OFAC restrictions. Christensen sits on the editorial advisory board of WorldECR.

Laurence Carey joins UTC
Well-known UK-based export controls professional, Laurence Carey has moved from Marshall Aerospace and Defence Group to US aerospace conglomerate United Technologies Corporation (UTC) in the UK. Before working at Marshall, Carey worked within the Aerospace and Defence Group at Deloitte. Laurence is a regular speaker at WorldECR Forum events.

Dual roles for Kevin Cuddy
On 8 February, GE Corporate’s Kevin Cuddy became the first trade, technology and security fellow at the Stimson Center, the nonpartisan policy research centre ‘working to solve the world’s greatest threats to security and prosperity’.

Cuddy will continue to work as senior manager of international trade compliance at GE in Washington DC, bringing in his new role ‘expertise in corporate export control and economic sanctions compliance to the world of non-proliferation to help improve industry and government connections and cooperation.’

The Stimson fellowship will examine how ‘evolving trade policies intersect with rapid developments in technology, as well as US security and foreign policy objectives.’

Kevin will be among the panelists at this year’s WorldECR Forum in Washington DC, to be held on 4-5 June.

Dutch merger
In the Netherlands, export control and sanctions specialists B&A Law have merged with regulatory and criminal enforcement firm, Wladimiroff Advocaten N.V.

B&A founders, Sebastiaan Bennink and Yvo Amar (pictured above left and right, respectively) explained the rationale behind the move: ‘Over the past years, our client base has grown considerably and it continues to grow at a very high pace. Since we want to be able to provide the same quality service and an even stronger enforcement practice in relation to sanctions and export controls, we have decided to merge with Wladimiroff, with whom we have already successfully worked on several enforcement cases.’

Amar was WorldECR’s Young Practitioner of the year in 2017.

Akerman acquisition includes Schulz and Manzanares
Akerman LLP has announced that it has ‘continued its Texas expansion’, hiring five international trade lawyers led by partners Michelle Schulz and Elsa Manzanares (pictured above left and right, respectively) who join from the Dallas office of Gardere Wynne Sewell. They are joined by Kim Carlson, Troy Shaffer and Matthew Savage.

Richard Spees, chair of Akerman’s Government Affairs and Public Policy Practice Group, said: ‘Michelle and her team are exceptional professionals who help clients navigate the most complex aspects of international trade, advocating for exporters and importers in US government investigations, fines and penalties, audits, disclosures, transactions and other trade matters.’

Lombardo takes the leap
California-based, former Dentons partner Kevin Lombardo has set up his own firm, Lombardo Law. The firm will focus on export ‘jurisdiction/classification, licenses/authorizations, audits (including due diligence), investigations of potential violations and implementing compliance programs,’ while on government contracts will assist clients with ‘internal investigations (usually relating to an alleged non-compliance with a contract or law), contract formation, technical data rights issues, compliance counseling, and disputes/claims.’
The WorldECR Awards 2018

The WorldECR Awards recognise outstanding work, vision, best practice, commercial benefit to the company, and contribution to international security, of organisations and individuals working in the fields of export control and sanctions compliance and non-proliferation.

WorldECR is pleased to invite nominations for the 2018 Awards. Nominations should be sent to Awards@WorldECR.com, to reach us by Friday 4 May 2018. Winners will be announced in our July 2018 issue.

Nominations – which can include self-nominations and need not be limited to one individual per organisation, and which are open to previous award winners – should be attached to your email and should include:

- Your name, position and contact details (email and phone)
- Name of the Award you are submitting for
- Name of individual/organisation you are nominating
- An explanation (up to 1,500 words) as to why your nominee deserves recognition in this Award category. (See categories below as to what the judges will be looking for; Please mark information as ‘Confidential’ where appropriate.)

The Award categories are:

1) **EXPORT CONTROLS COMPLIANCE TEAM OF THE YEAR – EUROPE***

2) **EXPORT CONTROLS COMPLIANCE TEAM OF THE YEAR – USA**

3) **EXPORT CONTROLS COMPLIANCE TEAM OF THE YEAR – REST OF THE WORLD***

For these awards, judges will look for outstanding performance on behalf of the company, excellence and innovation in the use of the team’s own resources, introduction and/or implementation of best practice in export control, and a positive contribution to international security.

4) **EXPORT CONTROLS LAW FIRM OF THE YEAR – USA**

5) **EXPORT CONTROLS LAW FIRM OF THE YEAR – EUROPE***

These awards recognise the law firm export controls team providing innovative work and valuable advice and representation to its client(s), assisting the function in its compliance efforts, and enhancing the function’s commercial contribution to its organisation. Judges welcome submissions highlighting an example taken from a variety of work, including advice on particular transactions, investigations and disputes as well as on regulatory issues.

6) **SANCTIONS LAW FIRM OF THE YEAR – USA***

7) **SANCTIONS LAW FIRM OF THE YEAR – EUROPE***

These awards will be given to the team that can demonstrate it provided the most impressive advice/representation on a specific Sanctions matter, or was instrumental in helping its client(s) through the fast-changing international regulatory Sanctions challenges of the past year. The winning firm will be able to demonstrate clearly the direct and positive effect and benefits to the client(s) of its advice.

8) **EXPORT CONTROLS/SANCTIONS LAW FIRM OF THE YEAR – REST OF THE WORLD***

This award will be given to the firm that can demonstrate it provided the most valuable advice/representation on Sanctions or Export Control matters, adding real and clear benefit to the business of its client.

9) **EXPORT CONTROLS CONSULTANT OF THE YEAR***

This award highlights the non-law firm export controls consultant or consultancy that has made the greatest contribution to its clients’ success in achieving export controls compliance, developing processes to future-proof systems and processes for its clients, and enhancing the export control function’s commercial contribution to its organisation.

10) **PRACTITIONER OF THE YEAR***

This award recognises truly exceptional individual contributions to the development and implementation of good practice in export controls and/or sanctions. The winner will have shown vision and either (1) great management skills and the ability to place their function in a position to deliver both commercial success to the organisation and greater security to the wider world and/or (2) to have pioneered new methods and/or thinking so as to significantly enhance the value of export controls and/or sanctions to the global community.

11) **YOUNG PRACTITIONER OF THE YEAR AWARD***

This award is open to export controls compliance and/or sanctions professionals in industry, legal private practice, consulting firms or government/regulatory bodies or NGOs. It recognises exceptional achievement on the part of an individual of 35 years of age or under.

* Europe Awards are also open to Europe-located offices/subsidiaries of non-European organisations
** USA Awards are also open to U.S.-located offices/subsidiaries of non-U.S. organisations
*** Rest of the world Awards are also open to U.S. and European subsidiaries located in Africa, Asia, Australasia and Central and South America
Canada plans to block controlled exports endangering human rights

No conclusive proof has emerged of Canadian vehicles being used in human rights violations by the Saudi government against its own people, but Ottawa will still take stock of its export control system. So said foreign minister Chrystia Freeland addressing a government committee on 8 February.

She also announced that the government would be supporting the inclusion of a ‘substantial risk clause’ in the law, by which government ‘would not allow the export of a controlled good if there were a substantial risk that it could be used to commit human rights violations.’ Freeland said: ‘[A] substantial risk clause would mean that Global Affairs Canada would need to ensure – before the export of controlled goods – that we have a high level of confidence that controlled exports will not be used to commit human rights abuses. ‘This is a significant decision. It will mean changes in how Canada regulates selling weapons. This is the right thing to do. Canadians fundamentally care about human rights for all, and Canadians rightly expect that exports are not used to violate human rights.’

Freeland also praised the progress the Canadian government was making with Bill C-47, which, when passed, will amend the Export and Import Permits Act to allow Canada to accede to the Arms Trade Treaty (‘ATT’).

Irish bill to ban business with occupied territories

A private member’s bill introduced to the Irish parliament would, if enacted, make it an offence ‘for a person to import or sell goods or services originating in an occupied territory or to extract resources from an occupied territory in certain circumstances.’

While not referring explicitly either to Israel or to the Palestinian territories, it has been drafted with the Gaza Strip and West Bank in mind.

The bill defines ‘relevant occupied territory’ as

‘a territory which is occupied within the meaning of the Fourth Geneva Convention, and which has been (a) confirmed as such in a decision or advisory opinion of the International Court of Justice, (b) confirmed as such in a decision of the International Criminal Court, (c) confirmed as such in a decision of an international tribunal.’

John Menton, partner at the law firm Arthur Cox, said that only a very small number of private members bills succeed in making it through the legislative process, and flagged a recent speech by trade minister Simon Coveney, who said: ‘Before I move on to the political issues raised by this Bill, I want to refer to legal aspects, because that has been mentioned. Issues of international trade fall under the common commercial policy of the EU. Under Article 3 of the Treaty on the Functioning of the European Union, TFEU, the common commercial policy is an exclusive competence of the Union. I have heard the argument that a public policy exception could apply to this Bill. However, I am advised that this argument is not well founded, and that the Court of Justice of the European Union interprets such unilateral restrictions on trade imposed by member states very narrowly.’

Coveney has also said that ‘the relentless expansion of Israeli settlements on Palestinian territory is unjust, provocative and undermines the credibility of Israel’s commitment to a peaceful solution to a conflict that we all want an end to.’

The Israeli embassy in Ireland has denounced the bill, which, it said, ‘only offers an incentive to those who wish to boycott Israel and stands in stark contrast to the guiding principles of free trade and justice.’

BIS grounds illegal supply of US parts to Iranian Airlines

The US Department of Commerce’s Bureau of Industry and Security (‘BIS’) has acted against a Turkish national and three Turkish companies over the supply of US aircraft engines and parts to Iranian airlines.

BIS has issued a temporary denial order (‘TDO’) to suspend the export privileges of Gulnihal Yegane, Trigron Lojistik Kargo Limited Sirketi, and affiliated companies Ufuk Avia Lojistik Limited Sirketi and RA Havacilik Lojistik Ve Tasimacilik Ticaret Limited Sirketi. Yegane was already on the BIS Entity List for supplying parts to designated Iranian airline Mahan Air.

‘Today’s action sends a strong message that trade with Iran in violation of U.S. export control laws and regulations will not be tolerated,’ said Commerce under-secretary Mira Ricardel. ‘The Bureau of Industry and Security will vigorously pursue parties that seek to take advantage of U.S. companies by providing false end-use information and that seek to profit from illegally supplying materials to Iran.’

Australia’s DFAT launches ambitious Defence Export Strategy

Australia’s Department of Foreign Affairs and Trade (‘DFAT’) has launched a new Defence Export Strategy, which aims to put Australia in the top ten defence exporters by 2028.

A major driver behind the move is job creation – a key policy for Prime Minister Malcolm Turnbull's government, which has already invested AUS$20bn in enhancing the capabilities of the Australian Defence Force (the army, air force and navy combined) as part of its 2016 integrated investment programme.

The Strategy does not propose any changes to Australia’s current export control laws, but rather new incentives, which are set to increase permit applications and requests for admission into the Australian and US ‘trusted trader’ communities.

‘We can see that Defence Export Controls (DEC – part of the Department of Defence) has already reconsidered its application requirements in line with the Strategy, making it mandatory to include estimated value as part of the item description, effective from December last year,’ said Alistair Bridges, a lawyer at the Melbourne office of Moulis Legal.

The new initiatives contained in the Strategy include a number of new administrative aids to help defence exporters, including an Australian Defence Export Office; a Defence Export Advocate and a Defence Export Facility, administered by Efic, Australia’s export credit agency, to help business with the financing of defence exports.

Investment of AUS$20m will be provided to implement the Strategy and support defence industry exports.

Part of that investment is likely to be funnelled into the DEC, which is responsible for approving defence exports. The Strategy’s provision of subsidies, easier credit and supportive collaboration between government and industry could also raise wider trade issues. ‘The line between security and trade policy can be difficult to define,’ said Bridges. ‘Although not exactly on point, the Trump Administration’s upcoming Section 232 decisions in steel and aluminium will give further insight into the degree to which the US feels import dependency impacts on national security. Our trading partners will have a hawk-like interest in these new developments.’

US senators propose sanctions against Cambodia

New legislation in the US would impose asset freezes, and prolong travel bans on members of the Cambodian government if the bipartisan sponsors of the Cambodia Accountability and Return on Investment (‘CARF’) Act of 2018 are successful in getting it enacted.

The law would build upon steps taken by the US government in December last year, when the State Department announced that ‘in direct response to the Cambodian government’s series of anti-democratic actions [including dissolution of the main opposition party and the imprisonment of Kem Sokha, head of the National Rescue Party] ... the Secretary of State will restrict entry into the United States of those individuals involved in undermining democracy in Cambodia.’

The proposed legislation would require continued implementation of the visa denial policy ‘until free and fair parliamentary elections have taken place, and provides for the freezing of assets of any individual captured by that policy.’

Regional media has reported that Sokha, who is awaiting trial on charges of ‘treason’ in Trapeang Phlang prison, has requested that he be transferred to Singapore for urgent medical treatment.

US senator Lindsey Graham said, ‘Democracy is dead in Cambodia today because the Cambodian government is under the influence and control of China,’ which he described as attempting to ‘colonise’ the country.

Fellow co-sponsor, senator Ted Cruz added that the legislation was ‘an appropriate response to Hun Sen’s protracted tyranny and unrelenting destruction of democracy in Cambodia. Kem Sokha remains imprisoned with the opposition party dismantled. How the United States responds to this authoritarian ploy will carry implications throughout the region. Hun Sen and his patrons in Beijing should not underestimate America’s resolve to preserve democracy in Cambodia and Asia.’

Further sanctions
The CARF Act also requires US executive directors of each international financial institution to oppose assistance to Cambodia until free and fair elections have taken place. Further, it authorises counter-influence programmes ‘to highlight China’s uniquely destructive role in that country during the 1970s, serving as a stark reminder to the Cambodian people that history should not repeat itself.’
US takes action against Latvia’s ABLV Bank for money laundering

The US Department of the Treasury’s Financial Crimes Enforcement Network (‘FinCEN’) has announced that it is seeking sanctions against Latvia’s ABLV Bank for money laundering.

FinCEN has issued a finding flagging ABLV as a primary money laundering concern, that has ‘institutionalized money laundering as a pillar of the bank’s business practices’. The lack of effective anti-money laundering (‘AML’), combating the financing of terrorism (‘CFT’) and sanctions policies and procedures have enabled illicit transactions, including for those connected with the North Korean ballistic weapons programme and ‘corrupt politically exposed persons’ funnelling billions of dollars through the financial system, said FinCEN.

FinCEN has also issued a notice of proposed rulemaking under §311 of the USA PATRIOT Act, which aims to cut the bank off from the US financial sector by prohibiting the opening and maintaining of a correspondent account in the US.

‘FinCEN’s recent notice about ABLV Bank reflects the ongoing and increasing use of special measures against financial institutions and other entities that US authorities believe are involved in activities inconsistent with US laws and foreign policy,’ said Keith Krakaur, a partner at international law firm Skadden. ‘If a financial institution or other entity avails itself of the US financial system, not having an adequate compliance programme significantly increases the risk that it may find itself in the cross-hairs, regardless of where it is based.’

The action follows FinCEN’s issue of a final rule against China’s Bank of Dandong in November 2017, severing the bank from the US financial system. The bank has been deemed to act as a gateway through which North Korea has accessed both the US and international financial markets, contrary to US and UN sanctions.

‘These sorts of designations are unlikely to have a big effect alone in either implementing the North Korean sanctions or in improving general anti-money laundering practices,’ commented DC-based Timothy O’Toole of Miller & Chevalier. ‘A single small bank designation is simply not large enough to make that happen on its own. However, when combined with significant publicity, the designations can suffice to get the word out to other, larger financial institutions that such practices carry extreme risks…..This was the strategy OFAC used in connection with Iran sanctions, and it eventually proved quite successful.’

World chess federation hit by OFAC sanctions

The world chess federation, FIDE, has announced that its bank accounts have been closed by its bank, UBS, on account of the presence on the OFAC SDN list of its former president, Kirsan Ilyumzhinov. Ilyumzhinov was also, between 1993 and 2010, the first president of the Republic of Kalmykia, formerly part of the Soviet Union.

In a 13 February letter to FIDE members, the organisation’s treasurer, Adrian Siegel, said that in 2015 Ilyumzhinov was placed on a sanctions list for facilitating purchases by the Syrian government of oil from ISIL.

In the same year, he withdrew from ‘any legal, financial and business operations of FIDE,’ despite which, wrote Siegel, ‘the Swiss bank UBS has announced that they will immediately close our accounts. The white money strategy in Switzerland does not allow business with institutions or persons on the sanctions list of the US Department of the Treasury … In summary, Kirsan Ilyumzhinov’s problems severely damage FIDE’s business activities and we have to look for a new bank connection.’

Not black and white
A tax lawyer in the office of a Zurich firm told WorldECR, ‘This was clearly a matter of internal policies and procedure. [The bank] evaluated the risk, and decided it wasn’t one that it wanted to take.’

He cautioned against attributing the account closure to Switzerland’s ‘white money’ strategy – initiated in 2013. ‘The white money strategy is a term of art – a policy of acting against circumvention of tax laws. It would not have had a bearing in this case,’ he said.
Eyes on the prize

In August 2017, WorldECR editor Tom Blass crossed continents to visit the James Martin Center for Nonproliferation Studies in Monterey, California, where he met the people directing the largest nongovernmental organisation in the United States devoted exclusively to research and training on non-proliferation issues. This is his report.

Notwithstanding all other considerations, it was almost fortuitous that I visited the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey (henceforth ‘CNS’ or ‘the Center’) in California in August last year, exactly as US-North Korean (or Donald Trump-Kim Jong Un) tensions were reaching their apex.

The forecast wasn’t good. A grey bank of mist rolled in off the Pacific, threats were being hurled between Pyongyang and Washington DC, and the world experienced once again the sense of nuclear dread which, most had hoped, had permanently abated shortly after the collapse of the Berlin Wall. It was fortuitous in so much as I was permitted an insight into the Center working at overdrive.

Quiet for a moment
CNS sits on a quiet street, seemingly a world away from the sealions, chowder stalls and candied excesses of Cannery Row. For much of the time, the department, scholarly and industrious, though very much engaged with the work of policymakers, government agencies and international institutions in the non-proliferation and nuclear security ‘space’, escapes the notice of the public at large. But over the course of that week last August, its experts were called into TV studios on almost an hourly basis, with journalists and anchor-men and women demanding answers to questions sometimes verging on the existential: ‘What is Kim Jong Un thinking? What is Donald Trump thinking? What kind of missiles does North Korea actually possess and what can they do? Are we on the brink of an apocalypse?’

CNS people are no strangers to the airwaves and international crises have a habit of setting their phones alight. Indeed, it’s safe to say that a surge in activity at CNS is not usually a positive indicator for the state of world affairs. Against this backdrop, I felt honoured that the Center’s programme director for export control and non-proliferation, Robert Shaw, had time to show me around the facility, and thankful to Robert and his colleagues for explaining their activities – which include research, outreach, training and diplomacy – as well as their raison d’etre.

Bringing it together
‘We really work,’ Shaw told me, ‘as a platform for bringing together stakeholders such as national governments and civil society, sometimes in closed briefings, and facilitating engagement between them. We run diplomatic workshops, host 1.5 track (backchannel diplomacy) meetings – and explore the potential impact of new and disruptive technologies such as biotechnology, or 3D printing.’

The Center, explains Shaw, also works to educate established and aspiring professionals, offering certificates and Master’s degrees in non-proliferation studies, and training in the use of new techniques for making the most out of tools such as 3D modelling, geo-spatial analysis and social media (the arrows in the quiver of the modern non-proliferation professional).

Its an organisation with a worldwide viewpoint and a global reputation. Alumni of CNS are known
in certain circles, as ‘the Monterey Mafia’, and they can be found in
governments and institutions across
the world.

Cold beginnings
The Center has its origins in work that
founding director Dr William Potter,
who kindly made time to meet with me
despite a busy schedule, was
undertaking in the late 1970s. (Dr
Potter’s next stop was lunch with
Lassina Zerbo, Head of the
Comprehensive Nuclear-Test-Ban
Treaty Organization.)

‘I was trained as a Soviet specialist.
That was the area of focus of my PhD at
the University of Michigan. Back then,
there were no “non-proliferation
studies”, although people like George
Quester and Joe Nye were writing on
the subject; actual university
programmes were as yet non-existent.’

Potter was struck by the parallels
between US and Soviet nuclear export
control policies: ‘What was remarkable
was the convergence of approach and
the level of cooperation between the
two at a time when the US and the
Soviet Union were at odds on
everything else. This was the period
that saw the London Group [now the
Nuclear Suppliers Group] created in
response to India’s nuclear test in 1974.
And it was a level of cooperation which
– with some caveats, such as the
signing of the JCPOA – has since
eroded. It doesn’t persist in the same
way.’

Potter conceived of the need for an
institution like CNS while undertaking
research into international nuclear
commerce at UCLA, which revealed
‘the apparent inability of the United
States government to readily track
international commerce in nuclear
commodities, including with respect to
transhipments and transshippers.’

With the end of the Cold War came
the ‘loose nukes’ crisis and the fear that
renegade (and hard-up) ex-Soviet
scientists would sell their expertise,
and possibly nuclear material, to the
highest bidder. In 1991 Potter reported
that in his estimation, over 100,000
people in the (then) Soviet Union could
have access to sensitive nuclear
information – he went on to organise a
meeting in Moscow in which he warned
of the risk of proliferation posed by
footloose scientists, a fear hardened by
an official from the ministry that ran
the nuclear complex, who confirmed
that its personnel had already been
approached by foreign recruiters.

The idea of the Center had always
been that it might be a hub for those
who shared these concerns but also for
creating methodologies by which
threats might be understood. ‘So, we
were the first to appreciate the need to
see individuals and companies as the
agents of commerce. Who’s involved
[in a transaction] who are the
individuals? But we had to train people
how to undertake these kinds of
analyses – and we were getting a lot of
interest in what we were doing from a
lot of different countries and
governments.’

From the outset, the Center decided
that it would only work with open
source data: ‘The Department of
Energy wouldn’t even share its
classified data with the Department of
State – but everyone could share ours!
We concluded that there is no
correlation whatsoever between what is
classified and what is accurate or
important!’ and henceforth, nurtured
the talent and the techniques that CNS
is using today.

A spirit of openness and
multilateralism generally appears to
have informed CNS’s future
development, enabling the Center to
build strong relationships across
national boundaries, with students
routinely finding internships and
employment in the international
organisations with which it has forged
partnerships.

To business
Unsurprisingly, with reputational and
financial penalties for sanctions and
export control breaches at an all-time
high, the Center is increasingly
successful at courting and engaging
with the private sector.

Robert Shaw has responsibility for
leading that charge. Shaw joined CNS
in 2010, having worked in export
control and supply chain management
for the previous decade, including as a
senior manager at Toshiba America,
where he was responsible for oversight
and implementation of internal export
control compliance within the
company’s procurement and export
division.

‘Currently,’ says Shaw, ‘there are
two vectors of engagement in the North
American context: both closely relate to
red flags. One area where we’ve been
active – alongside Kevin Cuddy at GE
– has been in organising discussion

CNS publishes a range of research
tools and materials

www.worldecr.com

10 WorldECR
and benchmarking roundtables, whose participants are senior-level trade/export controls specialists at technology producing firms.’

These roundtables, he says, typically draw around 15 representatives of industry. CNS will submit a ‘menu’ of topics to which it feels that it can add value: ‘Due diligence and red flags are invariably issues that come up for discussion, but we also look at the trends that are most current in non-proliferation and export controls, or, say, the intersection with IT security. Currently, there’s still a lot of focus on the Crimea-related sanctions and on avoiding diversion risk.’

‘Shaw, in these scenarios, would typically serve as a moderator and facilitator: ‘The key is letting the discussion flow. Where we provide input on the CNS side is sharing things that we’re observing or that we’ve heard in terms of proliferation threats and trends – it’s a means of direct outreach.’

These discussions – typically conducted over the course of a half or full day – give companies (who may, or may not be, competitors) an opportunity not only to share best practice but also to evaluate it – and to reach some kind of consensus as to what does or doesn’t work successfully.

Motivations are various. On the one hand, it is general risk reduction – with positive knock-ons for a company’s corporate responsibility portfolio. From an industry sector perspective, there’s also an opportunity to explore specific consequences of regulation, and to consider how best to develop compliance strategies accordingly. (As a paper prepared by Shaw and his colleague Catherine Dill notes, the incentive for industry participation here lies in ‘reducing the risk of a major export control or sanctions violation that might, if severe enough, result in legislative action adding constraints on an entire industry sector’s international trade activity – even if only one company perpetrated the violation.’)

For CNS researchers, the process assists in helping understand the extent to which companies, some of whom may be direct competitors, are willing to share their experiences with each other where or if they perceive a common interest.

Taking advantage of Monterey’s proximity to Silicon Valley, CNS also makes a point of participating in the regularly scheduled activities organised by the Northern California chapter of OWIT (‘The Organisation of Women In International Trade’).

‘Every other year, we present a full proliferation trend and red flag overview,’ says Shaw. ‘But we try to take it further. We’ve made a point of not just describing the proliferation environment and possible red flags but going beyond that, sharing our open source research methodologies. We’ve made a very conscious effort to move in that direction. Many companies are confident that they have their red flag detection methods up to speed. But what they want help with is ways of efficiently vetting “grey” flags – which, really, is the second level of due diligence.’

‘Both the approaches serve a critical purpose, in so much as that they provide an interface by which the highly specialised and frequently esoteric world of non-proliferation can engage with the compliance-focused world of business.

‘The overall goal is to attune industry to the proliferation environment, and to the kinds of diversion risk that technology companies can unwittingly fall prey to. The benchmarking roundtables and industry events help us to make sure that what we’re describing is not abstract and alien, but operationally useful. And that’s why my industry background was so appealing to the Center, because it helps immensely in helping make that translation.’

CNS also has resources, which, ironically, aren’t available to even hugely well-funded companies. ‘Fundamentally, most companies don’t have the research time to undertake extensive and painstaking due diligence, especially given the speed of the modern supply chain. They’re facing pressure to increase efficiency. But our research team has that time, and can spend days looking at satellite pictures, or at the shadows of buildings...’

For their part, Monterey researchers glean important insights, both into the extent to which companies are willing to share information with others, even competitors, but also around the efficacy and relevance of regulation.

‘A great deal of hard work goes into crafting policy, but it has to always be considered in an on-the-ground context. In the United States, and in other countries, such as the United Kingdom, the agencies do try to stay up to speed with the real nature of the threat. But it’s a challenge, and I think there are people who think that it needs attention. Good regulation reduces diversion but won’t choke off legitimate trade. But it can be a hit or miss thing. I’ve seen it, and I’ve heard from companies who say it. Some laws work. Others drain off time, and defeat their own fundamental goals!’

Korea moves...

No surprises that North Korea is currently preoccupying the James Martin Center. Taking time out from media appearances, research associates Melissa Hanham and Shea Cotton walked me through some of the open source tools they use to attempt to hone in on North Korean military capability, sanctions compliance – and procurement. Modern satellite imagery – and dogged ingenuity – have lead to some remarkable results. 3D modelling techniques, for example, have enabled CNS to undertake in-depth (open source) analysis of North Korea’s Punggye-ri nuclear site, to estimate the fuel capacity of North Korean ballistic missiles, and create models of Iranian centrifuges, so as to help verify compliance with the JCPOA.

Sometimes the outcomes are seemingly prosaic – but no less important for that: Hanham showed me a satellite picture of a khaki-clad crane, which evidently, had been used
for missile-lifting. 3D modelling allowed the team to identify the crane as not only being from Japan (and being on that country’s Commodity Watch List), but also, by determining its specifications, provide insight into the weight of the missile it was lifting. Another image enabled the team to trace a truck used to carry a missile in a display of military might to a manufacturer in China (it’s original purpose being hauling lumber).

Each revelation is like a piece of a jigsaw, helping make sense of a larger puzzle. ‘We’ve seen a significant increase of interest in our North Korea research in recent months and weeks, particularly from the Department of State and Department of Defense,’ says Shaw. ‘But beyond North Korea, what is driving our research strategically is to reduce the threat of proliferation. So, that means that you have to imagine a future in which there’s a potential breakthrough, that North Korea re-engages with the international community – a scenario like that which we’ve seen with Iran, although clearly that’s a work in progress. Still, if that were to happen, the work in the non-proliferation area will change. The expertise will certainly be required in any transitional period, just as currently, there’s a great deal of energy being expended on monitoring the implementation of the JCPOA. It would mean that there would need to be mechanisms in place on the Korean peninsula for decades.’

Watch the additives
It’s through organisation like CNS that the world – governments, businesses – become alive to new proliferation threats and fears – whether related to emerging technologies or new nuclear aspirations both from state and non-state actors.

Since I visited in August, CNS has been paying close attention to a development, the perception of which as a proliferation threat has waxed and waned but is currently seen as on point.

‘Export controls are well developed in terms of usual manufacturing processes, but the industrial and other possibilities opened up by 3D, or “additive” manufacturing, and its prominence in the supply chain is really going to create challenges.’

CNS has recently completed a project under a Department of Defense-sponsored grant to examine the proliferation implications of the technology, ‘...and also, who is using it – because you can’t separate the two.’ 3D printing is now ubiquitous,’ says Shaw, ‘not just in the well-resourced industrial domain, but it’s also accessibility by SMEs, entrepreneurs, and hobbyist communities that love experimenting with 3D printing. It offers enormous potential to the global economy and to human welfare, because in time it will enable people to manufacture almost anything, anywhere. It will lower the cost of production, and help developing economies get off the ground.’

But ‘almost anything’, of course, could be prosthetic limbs, or it could be export controlled rotors, vacuum pumps or machine tools – and may require a whole new paradigm of risk assessment, and fit-for-purpose regulation, if the proliferation threat is to be addressed.

‘We’re unlikely to be redundant any time soon,’ points out Shaw. ‘It would be nice to think the goal of eliminating proliferation is achievable. But somehow, I think that’s a way off.’
Arms and the Men

‘The nuclear arms control regime is in danger – and neither Vladimir Putin nor Donald Trump appear committed to saving it. Yet given enough political will, a solution could be found readily.’

Thus writes Steven Pifer, senior fellow in the Center for 21st Security and Intelligence, in a recent issue of the Berlin Policy Journal.

Pifer says that the Intermediate-Range Nuclear Forces Treaty (‘INF’) is under pressure from suspected Russian violations, and that were the INF to collapse, it would threaten the New START agreement, which requires the US and Russia to each reduce to no more than 1,550 deployed strategic warheads on no more than 700 deployed strategic missiles and bombers, which expires in 2021.

He notes that following the conclusion of New START in 2014, then-President Barack Obama proposed a new round of arms reduction negotiations that would include non-strategic nuclear weapons and non-deployed strategic weapons – meaning that for the first time, Washington and Moscow would negotiate on all nuclear weapons in their arsenals. Russian officials balked, citing concerns such as missile defence and conventional strike systems. They also called for the next negotiation to be multilateral, although the United States and Russia each maintain a nuclear arsenal that is more than ten times the size of that of any third country, and that since then, no further agreement has been possible.

‘Thus 2021 could see the end of negotiated limits on US and Russian nuclear forces, at a time when Russia is completing its nuclear modernization program and the United States is beginning to accelerate its planned modernization of its strategic delivery systems,’ says Pifer.

But there are steps that could be taken to restore confidence on both sides, he says. Each could allow the other the opportunity to scrutinise technology (e.g., Russia SSC-8 ground-launched cruise missile and the United States’ Aegis Ashore system) to reassure the other that they had not violated the INF. Also, Washington and Moscow could agree to extend New START until 2026: ‘That would preserve the treaty’s benefits and allow time for negotiation of a possible follow-on agreement. Of course, resolution of compliance concerns regarding the INF Treaty would create a much more positive atmosphere for consideration of New START’s extension.’

Creative thinking needed on counter-terror finance

In an article for the Royal United Services Institute (‘RUSI’), fellow Tom Keatinge and colleagues Florence Keen and Anton Moiseienko argue that ‘[I]n view of the terrorist threat and diversity of funding efforts, counter-terrorist financing efforts should aim to address the modus operandi of any given target, placing greater emphasis on the intelligence value that finance provides.’

They say that counter-terrorist financing (‘CTF’) is too frequently conflated with anti-money laundering (‘AML’): ‘CTF describes myriad activities, from the legal frameworks that countries put in place to prosecute terrorist finance and seize terrorist assets; efforts by financial institutions and other supervised entities to identify terrorist-related transactions, in accordance with law and regulations; and financial intelligence to inform the overall counter-terrorist picture.’

And they argue that it is ‘this final strand’ that is the most important, and yet it lacks prioritisation. ‘At its heart, it is the process of using financial intelligence to counter terrorism via law enforcement and the use of security services. Networks and associates, travel patterns and locations, communication methods, and purchases of vehicles or other materiel intended for use in attacks may all be identified through financial analysis. These contributions to the overall intelligence picture may be more valuable than simply removing one financial node.’

Models which developed in the wake of the 9/11 attacks should be revised in favour of ‘more creative thinking ... to meet the challenges of today,’ though such a rethink does not mean casting aside the current model: ‘The use of international sanctions and asset freezes to target high-level terrorist financiers and their networks should remain a core part of the global response, as should the reporting responsibilities of financial institutions. Greater emphasis must however be placed on complementary strategies that use financial intelligence to understand terrorist networks, including greater cooperation between law enforcement and private sector actors.’
The WorldECR Forum is moving ... from October to June.

- 4-5 June 2018: Washington, DC
- 28-29 June 2018: London

SAVE THE DATES

For all information, email WorldECR’s publisher at mark.cusick@worldecr.com
AUSTRALIA

Australian sanctions and export controls in the spotlight
By Alistair Bridges, Moulis Legal
www.moulislegal.com

On 17 December 2017, an Australian national – Choi Han Chan – was charged with breaching Australia’s nuclear non-proliferation laws, UN Security Council sanctions, and Australia’s autonomous sanctions. This represents the first time charges have been laid under Australia’s non-proliferation laws and autonomous sanctions.

There is currently little information as to the actions that have led to these charges. What is apparent is that it occurred between August 2017 and December 2017, and related to attempts to broker sales of various items from the Democratic People’s Republic of Korea (‘DPRK’).

Based on the charges, it is understood that Mr. Choi is alleged to have:

- Provided brokering services for the sale of missiles and related expertise in breach of Australian laws implementing UN Security Council sanctions against North Korea; and
- Attempted to transfer coal from the DPRK to entities in Indonesia and Vietnam in breach of Australia’s autonomous sanctions against the DPRK.

Australia’s nuclear non-proliferation laws broadly prohibit the provision of services that would or may assist a weapons of mass destruction programme without a permit or licence. Mr. Choi is also alleged to have breached this prohibition.

Offences under Australia’s sanctions laws – both UN originating and autonomous – can be punished with imprisonment for up to 10 years and fines equal to or greater than AUD525,000. Offences under Australia’s non-proliferation laws can be punished by imprisonment for up to eight years.

EU

EU Commission issues notice on Brexit impact on controlled goods
By Olivier Coulon, Loyens & Loeff
www.loyensloeff.com

On 25 January 2018, the EU Commission issued a notice regarding the impact of Brexit on future movements of controlled goods.

In its notice, the EU Commission recalls that, unless an agreement would provide for another date, the United Kingdom shall be treated as a third country as from 30 March 2019. The impact is expected to be significant, not only for the EU, but also and in particular for private parties, which are reminded here of the legal repercussions of the future Brexit.

Unless otherwise provided in a transitional agreement, different types of goods will be subject to import/export licences as from 30 March 2019. Amongst these goods are waste, certain hazardous chemicals, specimens of endangered species, rough diamonds, as well as dual-use and military goods.

While the notice is addressed to stakeholders engaged in shipments of goods subject to import or export licences, it is also of particular interest to entities engaged in transfers of controlled technologies. Private stakeholders dealing with the United Kingdom and controlled goods and technologies should plan ahead of 30 March 2019 so as to mitigate the future impact of Brexit. Increased compliance costs, triggered by heavier administrative procedures, are to be expected, together with potential uncertainties and slowdowns to be incurred in the beginning of 2019.
US Treasury releases list of Russian oligarchs and significant senior figures

By F. Amanda deBusk, Sean Kane, Alan G. Kashdan and Susie Park, Hughes Hubbard

www.hugheshubbard.com

On 29 January 2018, the US Treasury Department delivered a long-awaited but classified report to Congress identifying ‘significant senior political figures and oligarchs in the Russian Federation and Russian parastatal entities,’ as mandated by section 241 of the Countering America’s Adversaries Through Sanctions Act of 2017 (Pub. L. 115-44) (‘CAATSA’). At the same time, Treasury released a public version of the report identifying 114 political figures and 96 oligarchs that purported to rely on ‘objective’ criteria but was later revealed to have been derived in part from a Forbes magazine list of Russian individuals with an estimated net worth of greater than $1 billion, regardless of their links to the Putin regime.1

The same day, the US State Department announced that it would not, at this time, be imposing sanctions on any foreign entities for having engaged in ‘significant transactions’ with identified entities in the Russian defence and intelligence sectors, as mandated by section 231 of CAATSA. The State Department emphasised that 29 January was merely the first day that sanctions could be imposed under section 231 and that actions may be forthcoming. The two announcements show that the Trump Administration is taking an approach whereby it complies with CAATSA but does not go further than required.

Background on CAATSA

CAATSA was signed into law on 2 August 2017, authorising the imposition of new sanctions on Russia, Iran and North Korea. The Russia-related provisions of the law are the most far-reaching – in addition to codifying the sanctions regimes relating to Russia’s interventions in Ukraine and the 2016 US election, CAATSA significantly expanded the scope of secondary sanctions that could be imposed upon foreign persons engaging in certain transactions with or involving Russia.

The Administration has met most (though not all) of the statutory deadlines imposed by CAATSA since the law took effect. Most relevantly:

- In September and October 2017, the Treasury Department’s Office of Foreign Assets Control (‘OFAC’) amended the existing directives imposing sectoral sanctions on entities operating in Russia’s financial, defence, and energy sectors, tightening each in accordance with section 223 of CAATSA.
- In October 2017 – while weeks past the statutory deadline – the State Department issued guidance identifying 39 entities that are part of the Russian military and intelligence sectors, transactions which could result in the imposition of secondary sanctions under section 231 of CAATSA.

The Treasury and State Departments (which have been delegated authority under different provisions of CAATSA) have also issued several public guidance documents relating to their implementation of CAATSA, including:

- Section 223 (modifying the existing directives imposing sectoral sanctions)
- Section 225 (mandating sanctions relating to special Russian oil projects)
- Section 226 (mandating sanctions on Russian and other foreign financial institutions engaging in certain transactions)
- Section 228 (mandating sanctions relating to evasion and serious human rights abuses)
- Section 232 (authorising sanctions with respect to Russian energy export pipelines)
- Section 233 (mandating sanctions relating to investment or facilitation of privatisation of Russian state-owned assets)

Together, the guidance issued by the Treasury and State departments suggest the Administration has taken a cautious approach and preserved flexibility on implementation of the various provisions of CAATSA.

CAATSA section 2.41: The Oligarch Report

CAATSA section 241 required Treasury to submit a one-time ‘detailed report’ that included information about the relationship of the named individuals with Russian President Vladimir Putin or other members of the Russian ‘ruling elite’, their involvement in corruption, their net worth and sources of income, and the incomes and assets of their families. While the report itself was not a sanctions list, it was widely feared to signal potential future sanctions against named individuals.

However, by making public a report that indiscriminately identified all Russian billionaires, regardless of their ties to President Putin or their alleged involvement in corruption, the Administration appears to have been intent on stripping the report of any predictive value.

That said, the version of the report submitted to Congress is reported to be very different, and to directly identify individuals suspected of involvement in corruption or of having political

Links and notes

links to the Kremlin. It’s unclear why the Treasury Department decided not to make a version of that report public, even in redacted form, and the release of the public report so close to midnight on 29 January suggests that it was a point of contention within the Administration up until the very last minute. Regardless, the information included in the classified report to Congress – including identification of income sources and links to possible corruption – could provide the foundation for future sanctions. Congress is likely to take keen interest in the named individuals, and may use the report to exert pressure on the Administration to impose additional sanctions in the coming months.

**CAATSA section 231: Targeting Russian defence and intelligence**

As of 29 January 2018, CAATSA section 231 requires the president, acting through the State Department, to impose certain sanctions on persons determined to have knowingly engaged in a ‘significant transaction’ with specified entities in the Russian defence or intelligence sectors. The section gives the president the authority to waive or delay the application of sanctions on such persons if the president certifies to Congress that the Russian government has made significant efforts to reduce cyber intrusions or that the person is substantially reducing the number of significant transactions with the Russian defence or intelligence sectors.

Without specifically invoking either authority, the Administration declined to impose new sanctions under section 231 on 29 January. The State Department announced that the sanctions law was already acting as a ‘deterrent’ to those considering doing business with those Russian sectors, estimating that several billion dollars’ worth of Russian defence acquisitions by foreign governments have been abandoned since the enactment of CAATSA.

Although many viewed this development as a failure to aggressively enforce CAATSA, the Administration’s approach is not inconsistent with the language of the statute. Specifically, while Congress ‘mandated’ the imposition of such sanctions, the decision how to interpret ‘significant transactions’ and to determine that individuals or entities have engaged in them remains with the executive branch. Due to the chilling effect of the provision, many of the defence acquisition deals and relationships between foreign entities and the Russian defence or intelligence sectors were likely scrapped in the months since CAATSA’s enactment. Moreover, 29 January was only the first day that sanctions could be imposed under section 231. More revealing will be how and whether the Administration responds if major deals with identified entities in the Russian defence or intelligence sectors are announced in coming months.

**“US Export Controls on Non-US Transactions”**

NEW EAR & ITAR Definitions and all Reform Changes

**EAR / ITAR & OFAC COMPLIANCE FOR NON-US COMPANIES**

COMING TO:  
SINGAPORE • LONDON • WASHINGTON DC • AMSTERDAM  
MARCH 2018 • MAY 2018 • JUNE 2018 • OCTOBER 2018

- Persons and Items Subject to US Jurisdiction (ITAR, OFAC & EAR)  
- United States De Minimis Content Calculation  
- Trump Administration Regulation and Enforcement Priorities  
- Technical Data Considerations  
- Enforcement Issues, Practical Advice…and MUCH MORE

Visit [www.LearnExportCompliance.com/schedule](http://www.LearnExportCompliance.com/schedule) or call +1 540 433 3977 (USA) for details or registration
The petitioners have asked the Department of Commerce to expedite the investigation and for the president to impose quota restrictions on uranium products from Russia. Specifically, they seek to reserve 25% of the US market for domestic uranium and a requirement for US government agencies to purchase uranium from domestic sources.

Senator John Barrasso (R-WY) also asked for Commerce to launch an investigation under section 232 on the effects of uranium imports on national security. According to the US Senate Committee on Environment and Public Works, uranium from state-subsidised companies in Russia, Kazakhstan, and Uzbekistan, provides approximately 40% of US uranium. Barrasso argues that the United States, however, produces less than 5% of the yellowcake (uranium oxide) it consumes, with the majority of US uranium production in Wyoming.

Ur-Energy and Energy Fuels Resources signed a joint petition on 16 January regarding imports of uranium from state-owned and state-subsidised companies primarily in Russia, Kazakhstan, Uzbekistan, and possibly China. The petitioners claim that ‘[the United States] cannot afford to depend on foreign sources – particularly Russia, and those in its sphere of influence, and China – for the element that provides the backbone of our nuclear deterrent, powers the ships and submarines of America’s nuclear Navy, and supplies 20 percent of the nation’s electricity.’

The petitioners have asked the Department of Commerce to expedite the investigation and for the president to impose quota restrictions on uranium products from Russia. Specifically, they seek to reserve 25% of the US market for domestic uranium and a requirement for US government agencies to purchase uranium from domestic sources.

Senator John Barrasso (R-WY) also asked for Commerce to launch an investigation under section 232 on the effects of uranium imports on national security. According to the US Senate Committee on Environment and Public Works, uranium from state-subsidised companies in Russia, Kazakhstan, and Uzbekistan, provides approximately 40% of US uranium. Barrasso argues that the United States, however, produces less than 5% of the yellowcake (uranium oxide) it consumes, with the majority of US uranium production in Wyoming.

An investigation on uranium imports would be the third probe under section 232 of the Trade Expansion Act of 1962 since President Trump took office early 2017. Commerce Secretary Wilbur Ross submitted the section 232 list – and any transactions that might expose themselves to sanctions under CAATSA.
The future is now (or, at least, soon)

Slaughterbots – a not terribly pleasant but fairly convincing (fictive) video available on YouTube, paints a picture of a not distant future in which tiny, unstoppable, killer drones are so cheap to manufacture as to be ubiquitously available to terror groups and other non-state actors. (They kill, by the way, by planting explosive charges on the foreheads of their victims. Ouch.)

Most of the technology that these (as yet non-existent) machines utilise is already commonplace. The drones themselves are outwardly the same as those wedged in so many Christmas stockings this year. Facial recognition is a reality, as is the ability to track targets and avoid obstacles – notwithstanding the odd Google Car bump.

The danger that its authors want to highlight is fairly obvious: these things are imminent; the world should preemptively ‘strike’ with a global ban on autonomous weapons.

But the video has kicked off something of a (polite) storm in the policy world. Yes, say critics, the reality of ‘slaughterbots’ may be around the corner. But there are very many other kinds of technology, including the UAVs used by the US government to lethal effect in Afghanistan, Yemen, Pakistan and elsewhere, which have yet to find their way into the arsenals of non-state actors.

It is a provocative discussion which strikes at the heart of questions around the regulation of technology. What kinds of product are so unconscionable that, once conceived of, should never be permitted to exist? And from a more prosaic perspective, what steps should business be taking to anticipate such developments, given the tendency of the present to gallop toward a sci-fi future?

We cannot promise that the answers to this question (and others, such as the correct way to prepare for Brexit, the future of key sanctions programmes, the impact of data tools on export controls and sanctions compliance and very many more) will be delivered, neatly packaged, to delegates attending the WorldECR Forums in Washington and London this June. But we do promise healthy and extremely informative discussion and debate upon the topics – both enriching, and enlivening.

Expect the programme in your inbox shortly.

The video (you’ll never see your children’s toy drones in the same light ever again) is at: https://www.youtube.com/watch?v=9CO6M2HsoIA

Tom Blass, February 2018
TNB@worldecr.com

Raphaël Barazza
Avocat à la Cour

33 rue Galilée, 75116 Paris, France
Phone + 33 (0) 1 44 43 54 63
www.customs-lawyer.fr
Demystifying delisting: A guide to seeking removal from international sanctions lists

The increased use of sanctions by international powers has created long lists of designated parties who can quickly find themselves trapped by their listing. Dr. Anna Bradshaw, Barbara Linney, Collmann Griffin and Alice Kemp examine the differing methods for challenging a listing under the UN, US, EU and developing post-Brexit UK regimes and the strategies offering the greatest chance of success.

Over time, the United Nations, the European Union, and many of their member states, including the United States, the United Kingdom, and numerous other countries, have expanded their use of sanctions as a foreign policy tool, generating ever longer lists of individuals and entities subject to sanctions. Each jurisdiction has its own procedures for both adding names to the lists and addressing removal petitions. Adding to the complexities facing persons seeking removal from multiple lists, with ‘Brexit’ on the horizon, the United Kingdom is in the process of establishing its own separate mechanisms for persons seeking delisting from UK lists, and this process has shed light on the ongoing debate regarding the sufficiency of procedural rights protections available to targets of sanctions.

In this article, the authors compare the UN, EU, US and the nascent post-Brexit UK procedures for challenging a sanctions list designation (listing) and seeking removal from the relevant list (delisting).

Not surprisingly, while persons seeking delisting face both procedural and substantive hurdles in all jurisdictions examined by the authors, the US system poses the most significant obstacles to delisting, especially for non-US sanctions targets. Moreover, given the need to seek removal from multiple lists, the authors emphasise the need for a coordinated approach in order to achieve meaningful results.

Delisting at the United Nations
The United Nations Security Council currently administers 14 sanctions regimes. Most of these sanctions programmes feature arms embargoes, travel bans, and asset freezing, and each is administered by a separate sanctions committee consisting of Security Council members and supported by a ‘Group of Experts,’ ‘Panel of Experts,’ or ‘Monitoring Group’ appointed for that purpose by the appropriate committee. Active sanctions committees include the ‘ISIL (Da’esh) & Al-Qaida Sanctions Committee’ (‘ISIL & Al-Qaida Sanctions Committee’), the ‘1718 Sanctions Committee,’ and the ‘Somalia and Eritrea Sanctions Committee,’ among others. Parties that find themselves listed under a UN sanctions regime have two procedural tracks for delisting (or for petitioning for a humanitarian exemption, available under some programmes). An individual petition may be filed by a listed party with one of the offices the UN Security Council has established to handle delisting petitions: the Office of the Ombudsperson for the ISIL & Al-Qaida Sanctions Committee, which manages delisting petitions for the ISIL & Al-Qaida sanctions regime, or the Focal Point for Delisting, which manages delisting petitions for all other UN sanctions regimes. Alternatively, a listed party may petition the UN member state of citizenship or
Sanctions delisting

making procedures. Individuals or entities seeking delisting may submit petitions directly or through a representative to the Office of the Ombudsperson, who will report to the committee and make a recommendation regarding the delisting request. If the ombudsperson recommends continuing the listing, it typically will remain in place. A recommendation to delist will be handled by the committee in the same manner as a petition from the member state(s) that proposed the listing.

In contrast, for delisting petitions before other sanctions committees, the Focal Point for Delisting acts more as a coordinator, acknowledging the receipt of the petition and forwarding the petition to the reviewing member states, which consist of the designating government(s) and the member states of the petitioner’s citizenship and residence. After a review period of three months or more, these reviewing governments will notify the Focal Point whether they concur with or object to the petition (or have no comment), and the matter is referred to the appropriate committee for decision.

Substantively, grounds for delisting include no longer meeting the listing criteria under a particular sanctions regime or the mistaken identification or death of the petitioner. Sufficient documentation should be provided for the petitioner to support his or her claim, for example, by countering the reasons for listing stated in the list entry for the petitioner.

As discussed below, whether the UN review mechanisms provide sufficient procedural protections for petitioners is a matter of ongoing debate.

UK and EU perspectives

Proposed legislation for post-Brexit UK sanctions in the Sanctions and Anti-Money Laundering Bill has focused attention on the scope of ministerial discretion to designate, and forced a timely revisiting of the basis on which designations should be susceptible to challenge. Questions are being raised about the sufficiency of the proposed review mechanisms and extent to which they might represent a ‘step backwards’ from the remedies presently available under the EU system.

These concerns tie in with a larger debate, at UN level, about the sufficiency of procedural rights protections available to targets of sanctions. It is no secret that the UN review mechanism is less sophisticated than the EU’s; the development of the latter has undoubtedly benefited from being subject to the jurisdiction of the Court of Justice of the EU (‘CJEU’), as demonstrated by the seminal decision in Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, cases C-402/05 P and C-415/05 P. Whilst the procedural protections available to sanctions targets in the European Union still fall far short of those available on a criminal charge, a number of important concessions have been made. It is feared that a failure to similarly address the ’rights deficit’ at the UN level could undermine the perceived legitimacy of UN sanctions.

Against this background, it is ironic that the model now proposed for future UK sanctions legislation approximates the UN rather than the EU model. A further issue which has not yet received much attention is the increased prospect of conflicts of laws, and inconsistent application of international human rights norms, arising from the parallel operation of self-contained listing regimes within a relatively confined geographical area, under which the same natural and legal persons could potentially be treated very differently. Those advising designated persons in the UK are already experienced in navigating three separate delisting regimes depending on whether the designation was made by the UN Security Council, ‘autonomously’ by the EU Council, or unilaterally by Her Majesty’s Treasury. Once the United Kingdom leaves the EU (and any transitional period has expired), there will be two more domestic review mechanisms added into the mix. These are, of course, all supplemented by extraneous routes for indirect challenges to listings; attacking the compatibility of sanctions legislation with competing international law obligations –

It is no secret that the UN review mechanism is less sophisticated than the EU’s.

Links and notes

2 See UNSC Res. 1718 (imposing sanctions on the Democratic People’s Republic of Korea (DPRK)).
4 See UNSC Res. 1730 (2006).
5 R (Breidenkamp) v Secretary of State for Foreign and Commonwealth Affairs [2012] EWHC 3297 (Admin).
7 Mustafa v HMT [2012] EWHC 3578 (Admin).
9 Application No 58090/08, Grand Chamber, 21 June 2016
10 31 C.F.R £501.807.
11 Although 31 C.F.R §501.807(a) requires a written application to be mailed, guidance available on OFAC’s website permits submission via email. See https://www.treasury.gov/resourcecenter/sanctions/SDNListOfPages/petitions.aspx (last visited 16 February, 2018).
12 Id.
13 Id.
14 Id.
16 31 C.F.R. § 501.807(a).
19 Epsilon Electronics, Inc. v. United States Dep’t of Treasury, 857 F.3d 913, 925 (D.C. Cir. 2017).
22 Epsilon Elecs., 857 F.3d at 927.
23 KindHearts, 647 F. Supp. 2d at 872.
24 See, e.g., Al Haramain Islamic Found., Inc. v. U.S. Dept of Treasury, 886 F.3d 965, 985 (9th Cir. 2015).
including the possibility of initiating proceedings before the European Court of Human Rights, the International Court of Justice or the WTO dispute settlement mechanism, or approaching a UN treaty-based committee or the Human Rights Council.

**EU delistings**
Designations imposed by EU restrictive measures can be challenged administratively by writing to the Council’s General Secretariat, and in annulment applications brought before the General Court. The two avenues of challenge are not mutually exclusive and are necessarily pursued in tandem, in order to avoid the risk of the Council not responding within the strict deadline for bringing an annulment application (two months and ten days following a listing or a renewal of a listing). Despite the relative strengths of the EU mechanisms for challenging designations as compared to the corresponding UN mechanisms, neither remedy is without its critics.

*The availability of an EU remedy excludes a national remedy*

There is, in theory, no recourse for challenging EU restrictive measures at the national level. The UK courts have nevertheless seen challenges mounted against domestic actions taken in connection with the implementation and enforcement of the EU designation. Examples include the UK government’s participation in nominating and maintaining a listing5 and, famously in the Rosneft case,6 challenges to the national legislation criminalising breaches of EU restrictive measures and guidance issued by national authority on their interpretation. A strategic advantage of bringing proceedings in the domestic court is the prospect of a request for a preliminary ruling by the CJEU on a matter of interpretation (as in Rosneft), pursuant to article 267 of the Treaty on the Functioning of the European Union (‘TFEU’); which would result in the highest judicial authority in the European Union considering the case before any related annulment application is likely to be determined by the (lower instance) General Court. However, the current reluctance on the part of the UK judiciary to request preliminary rulings as Brexit looms makes the UK courts an increasingly unattractive proposition for such proceedings.

**Practical obstacles**
Both remedies should, in theory, be equally accessible across the European Union, although some EU Member States may prove more accessible than others in practice, depending on the designated person’s personal circumstances.

Those who seek to challenge their EU designations face a number of practical obstacles; the biggest of which is likely to be cost, particularly for those ineligible for legal aid. The great majority of sanctions targets are located outside the EU, and many, if not most, will have limited financial means. Whilst an administrative review process can in principle be engaged without the assistance of a lawyer, identifying legal arguments and the necessary supporting evidence might be an unachievable feat for all but the most resourceful designated persons.

An EU-qualified lawyer will be even more indispensable for bringing annulment proceedings in the General Court; the costs of which will be exacerbated by the length of the proceedings. Well-established derogations from asset freezes permit designated persons to access their funds for reasonable legal expenses, but Member States’ competent authorities vary in their approaches to deciding applications. In practice, access to justice can easily be obstructed by the time taken to process applications, the nature and amount of supporting information requested in support of an application and limitations imposed on the amount of permitted expenditure.

**Substantive obstacles**
The bar for a successful challenge...
UK-only terrorism designations can currently be challenged only by way of appeal in the High Court. There is no administrative route.

Unilateral terrorist listings

UK-only terrorism designations can currently be challenged only by way of appeal in the High Court. There is no administrative route. (like the EU court) grappled with the extent to which procedural protections should be made available to designated persons; with debate focusing principally on the extent to which sensitive material relied on in support of the designation can be withheld from disclosure. An ‘irreducible minimum’ of disclosure is required in order for an appellant to have a fair hearing compatible with article 6 of the European Convention on Human Rights. The court can consider ‘closed’ material not accessible to the designated person or their lawyer, but must in each instance carefully consider the extent to which public interest requires disclosure and whether any concessions would need to be made in order to ensure a fair trial.

Post-Brexit listings

The Sanctions and Anti-Money Laundering Bill proposes two new review mechanisms that can be invoked by designated persons, broadly mirroring the existing EU administrative and legal remedies. Each remedy can only be exercised once, unless there is a significant matter which has not previously been considered; a limitation which, according to the explanatory notes, is intended to guard against vexatious repetition.

The administrative remedy is more limited for designations made pursuant to a UN obligation, as a UN-designated person can only request that the secretary of state uses ‘best endeavours’ to secure the removal of the name from the UN list in question. By contrast, persons subject to unilateral UK designations can request the minister that made the designation to revoke it, or to vary it in light of changed circumstances. A designation must be revoked if the conditions on which it was based are no longer met, irrespective of any request to do so; but it is otherwise left entirely to the minister’s discretion whether to vary or revoke the designation, or to take no action in response to a request. The position is broadly the same for persons who are designated under retained EU autonomous sanctions during the two-year transitional period: ministers must direct that a name be treated as removed from the list if there are no reasonable grounds to suspect that the person satisfies the conditions for listing under the EU sanctions in question, or if the minister does not consider it appropriate for the person to remain designated.

Unlike under the existing EU regime, the administrative route must be exhausted first before the court can be approached, in order to minimise ‘unnecessary’ litigation. The absence of any time limits for responding to requests led to concerns that ministers could delay recourse to a court by failing to respond in a timely manner. Amendments introduced to the bill would require ministers to determine requests as soon as reasonably practicable after receipt of the information needed for making the decision. Ministers would also be required to inform the person who made the request of the decision and the reasons for it as soon as reasonably practicable. Whilst a broad range of ‘sensitive’ information can be withheld the minister must provide some reason, rather than none at all.
Recourse to the UK courts is by application to set aside decisions made by ministers on administrative requests or otherwise in connection with the administration of the sanctions regime. There is no recourse to ordinary judicial review: the same principles will be applied, but in a modified procedure under which sensitive ‘closed material’ may be heard in the applicant’s absence and without the ability to award damages other than for negligence or decisions made in bad faith.

**Future uncertainty**

It remains to be seen whether the mechanisms for challenging post-Brexit sanctions will prove to be effective remedies, in practice as well as in theory. The answer will depend in no small part on the policy approach that ministers take to legal expenses licence applications. Whatever the position adopted, it is likely to reflect a difficult balancing act; the UK regime must be robust enough to withstand legal challenges, but without appearing to be a strategically more advantageous forum for pursuing challenges in than the European Union.

A key question will be whether the proposed UK review mechanism will be considered sufficient to satisfy even the comparatively low expectations of the European Court of Human Rights, by whose jurisdiction the UK will continue to be bound post-Brexit. As confirmed in *Al Dulimi and Montana Management Inc v Switzerland,* whilst UN member states are under a legal obligation to comply with Security Council Resolutions, they should nevertheless ensure that there is a review mechanism in place sufficient for designated persons to satisfy themselves that listings adopted by the Security Council are (at the very least) not arbitrary.

A more complex question concerns the interplay between EU and UK listings and delistings; for example, where there are dual or ‘double’ designations based on the same supporting material but parallel challenges lead to disparate outcomes.

What is the practical significance of a delisting in one regime, where the listing remains in the other, given that cross-border businesses are likely to be either bound by or voluntarily abide by both? The issue is likely to arise immediately, even during the two-year transitional period, as the bill makes provision for UK ministers to remove or add people to EU sanctions ‘retained’ pursuant to the separate withdrawal legislation (the European Union Withdrawal Bill 2017-19).

**Delisting in multiple jurisdictions**

Persons seeking delisting in one jurisdiction have often been listed in other jurisdictions as well. As a practical matter, therefore, it may be prudent to pursue delisting in all relevant jurisdictions simultaneously. In this regard, it is important to remember that while the United States is obliged to implement the UN Security Council resolutions, most additions to the SDN List that are designed to comply with the UN Participation Act are also authorized under other sanctions authorities, with the result that delisting at the UN level will not lead to automatic delisting by the United States. Furthermore, particularly if the delisting petition is brought on the basis of changed behaviour such that listing is no longer warranted, the support of a permanent member of the UN Security Council such as the United States or the United Kingdom may well enhance a petitioner’s likelihood of success before the United Nations.

**Delisting in the United States**

The United States maintains lists of persons subject to primary and secondary sanctions. In general, primary sanctions are enforced by the Office of Foreign Assets Control of the US Department of the Treasury (‘OFAC’), which administers a list of persons subject to asset blocking (or ‘freezing’) with whom US persons may not deal – i.e., the List of Specially Designated Nationals and Blocked Persons (‘SDN List’) – and a list of persons subject to sectoral sanctions – i.e., the Sectoral Sanctions Identification List (‘SSI List’). To the extent that secondary sanctions imposed against an individual or entity consist solely of asset blocking and related travel bans, such persons are listed on the SDN List. However, other secondary sanctions lists are maintained by the US Department of State.

OFAC’s regulations provide for administrative reconsideration of designations as blocked persons (i.e., petitions for removal from the SDN List).\(^{10}\) The regulations do not stipulate a formal procedure for reconsideration of SSI designations, but OFAC officials have stated that the same process can be used to seek removal from the SSI List as well. On the other hand, there are no procedures governing delisting from the various secondary sanctions lists maintained by the Department of State, but in practice petitioners may seek relief from the bureau responsible for the applicable listing.

Procedurally, OFAC’s administrative review process is relatively simple. The process begins with a request for delisting, either through post or email.\(^{11}\) Although successful petitions must contain enough information to counter OFAC’s own evidence for listing, as a formal matter...
OFAC is subject to judicial review by US courts, although the degree of procedural protection afforded non-US petitioners falls short of the protections available to US persons.

Petitions and questionnaires, including delays that have led to delisting matters that last months or years. Substantively, OFAC states that it will consider delisting when ‘insufficient basis exists for the designation,’ as well as when there are ‘remedial steps’ on the part of the blocker person, ‘such as corporate reorganization, resignation of persons from positions in a blocked entity, or similar steps, which the person believes would negate the basis for designation.’

However, the OFAC removal guidance states that OFAC also will consider delisting when there is evidence of ‘a positive change in behaviour, the death of an SDN, the basis for the designation no longer exists, or the designation was based on mistaken identity.’

Furthermore, as explained below, OFAC is subject to judicial review by US courts, although the degree of procedural protection afforded non-US petitioners falls short of the protections available to US persons.

If OFAC denies a delisting petition, the blocked person may either reapply to OFAC with additional information or new evidence of remediation or challenge OFAC’s action in court. As a general matter of US law, a court can only review an action by an administrative agency such as OFAC if that action constitutes a ‘final agency action,’ which the US Supreme Court has defined in non-OFAC related cases as an action that ‘mark[s] the consummation of the agency’s decision making process’ and is not ‘of a merely tentative or interlocutory nature’.

However, challenging a listing in the US courts typically will be ineffective if based solely on OFAC’s policy choices and evidence-based factual determinations. US courts generally are deferential to administrative agencies on matters of policy within an agency’s area of expertise, particularly when that area of expertise is national security. Furthermore, US courts also generally are deferential to OFAC’s findings of fact, so long as such findings are supported by ‘more than a scintilla’ of evidence. Finally, US courts generally are willing to accept OFAC’s reliance on classified data to which the petitioner likely does not have access, or even hearsay and unverified, open-source information from newspapers.

Nevertheless, an appeal to the US court system may be effective when OFAC has committed some sort of procedural error. Almost all of the successful challenges to OFAC’s authority, both within the delisting context and in other contexts, have focused on such defects. For example, litigants against OFAC have prevailed in court when OFAC failed to provide a reason for discounting evidence contrary to its conclusion, when long delays render OFAC’s decisions unfair, or when OFAC’s actions are deemed to violate a petitioner’s constitutional rights, to the extent that a non-US petitioner enjoys such rights. Therefore, although delisting may be generally an administrative process, petitioners should be alert to procedural defects that could permit litigation in US courts. However, as in the United Kingdom, petitioners who are successful before the courts may simply find themselves back before OFAC, which will have an opportunity to reissue its decision on amended grounds.
OFAC’s pivot to Asia: new risks emerge

Recent events suggest that OFAC’s appetite for enforcing US secondary sanctions should be putting East and Southeast Asian companies with commercial ties to Iran and North Korea on alert, writes Sean Kane.

In the past, European financial institutions and businesses were not always sensitive to the reach of US sanctions. The US Department of the Treasury’s Office of Foreign Assets Control (‘OFAC’), which administers and enforces most US sanctions, as well as other regulators and prosecutors, occasionally targeted enforcement action at the prohibited re-export of US controlled goods, technology and services to embargoed jurisdictions such as Iran and Sudan, but historically most civil and criminal enforcement of US sanctions was directed at US individuals and entities. Similarly, until the early 2010s, sanctions imposed on specific parties most commonly targeted individuals and entities located in, and with direct links to, sanctioned countries (e.g., the blocking of Iranian entities or of Cuban nationals).

That landscape changed dramatically within the last decade. First, a series of new legislative and executive authorities allowed OFAC to impose sanctions on third-country firms engaged in transactions that had no nexus to the United States. Sometimes called ‘secondary sanctions’, these authorities proliferated most dramatically in the context of Iran, and the threat of such sanctions went a long way in severing Iran’s access to EU markets.

Second, OFAC (among others) began to focus its enforcement action on EU financial institutions that, through their alleged misconduct, undermined US primary sanctions regimes by allowing prohibited parties to access the US banking system by routing dollar transactions through New York-based banks, while often concealing the sanctioned country component of the underlying transaction. Sometimes referred to as the ‘big bank’ cases, they culminated in 2014 with BNP Paribas’s combined $8.9 billion settlement with federal and state agencies (including a record $963 million agreement with OFAC) for apparent violations of US sanctions.

As a consequence, many of Europe’s biggest banks and companies have now adopted compliance policies that use US sanctions prohibitions as their baseline. East and Southeast Asian firms, however, are only just beginning to appear on OFAC’s front line for enforcement, as demonstrated by a handful of high-profile actions in 2017. This suggests there is comparatively little sensitivity to US sanctions within the region. Combined with the US government’s new emphasis on targeting North Korea’s access to international markets, as well as the potential for renewed emphasis on Iran, the risks and potential exposure for Asian firms have never been higher.

Asia’s exposure to high-risk markets

East and Southeast Asian firms are particularly vulnerable because of their commercial links to Iran, North Korea, and to a lesser extent, Russia. East and Southeast Asian firms are particularly vulnerable because of their commercial links to Iran, North Korea, and to a lesser extent, Russia. While US companies are broadly prohibited from directly or indirectly engaging in transactions with Iran and North Korea, and the biggest EU firms and financial institutions remain wary of engaging in even authorised transactions with countries subject to US sanctions, East and Southeast Asian businesses are increasing their
Iran

The US and EU campaign to cut off Iran’s oil exports in 2011-2012 was largely successful in significantly reducing potential markets for Iranian oil. In 2011, Iran exported an estimated 2.6 million barrels per day of crude to buyers in Asia and Europe, but in 2014 that number nearly halved, to 1.4 million. That reduction was primarily borne by the EU, which prohibited imports of oil from Iran. Threatened with secondary sanctions, many Asian countries agreed to reduce their imports of Iranian crude, but never eliminated such purchases entirely. As a result, Iran became increasingly reliant upon East and Southeast Asian markets – primarily China, Japan, South Korea, and Taiwan.

That trend line continued after international sanctions were relaxed under the Joint Comprehensive Plan of Action (‘JCPOA’) agreed in 2016 by Iran and the members of the United Nations Security Council, plus Germany (the ‘P5+1’). China is now the largest buyer of Iranian oil and Asia the largest export market, accounting for an estimated 60-70% of Iranian crude exports in 2017, even though such purchases are no longer prohibited for countries outside of Asia under UN or EU sanctions (US primary sanctions still prohibit sales to the US or transactions involving the US dollar). Iran has actively promoted such ties, offering discounts to existing buyers in Asia in order to boost its market share within the region.

The commercial links between East and Southeast Asia and Iran are not limited to oil imports. Major Chinese, South Korean, and Japanese firms have recently made significant investments in Iran’s energy and shipbuilding industries, and with increasing business activity comes all of the attendant financial services. Further, because the international sanctions regime prior to the JCPOA largely inhibited Iran from selling oil for western currencies, much of Iran’s oil trade with Asia during that period was settled in goods. The inroads made by Chinese and South Korean exporters in exporting such goods has not abated – studies estimate that China alone now accounts for between 50% and 100% of Iran’s imports of textiles, iron, and steel.

North Korea

United Nations sanctions on North Korea have progressively curtailed that country’s import and export markets. UN member states are now prohibited from importing North Korean coal, iron, lead, precious metals, and seafood, among other items, and exports of crude oil and refined petroleum products to North Korea have been severely limited. Official statistics reflect that these sanctions are having a material impact – overall Chinese trade with North Korea was estimated to have dropped 10.5% in 2017 (although China continues to account for the overwhelming majority of North Korea’s imports and exports). India, Pakistan, Thailand, the Philippines, and Russia – which together account for the remainder of North Korea’s import and export markets – have also reported declines. Despite the official statistics, North Korea continues to use front companies and other illicit measures (such as ship-to-ship transfers of oil in international waters) to access critical goods, financial services, and hard currency. Those efforts are heavily concentrated in East Asia, especially China.

Highlighting those persistent links, in November 2017 the US Department of the Treasury’s Financial Crimes Enforcement Network (‘FinCEN’) imposed correspondent banking restrictions on China’s Bank of Dandong, alleging that it served as a conduit for illicit North Korean financial activity, and in January 2018 OFAC announced sanctions against China-based Beijing Chengxing Trading Co., Ltd., and Dandong Jinxiang Trade Co., Ltd., alleging they had been involved in the export of metals and technology for use in North Korea’s missile programme.

At least in the eyes of the US government, East Asia remains North Korea’s primary outlet to international markets.

Secondary sanctions authorities

East and Southeast Asia’s commercial ties to Iran, North Korea, and Russia pose a significant risk that businesses in the region will be targeted under US secondary sanctions authorities. Critically, such authorities do not depend upon the involvement of US banks, the re-export of US products or services, or the evasion of US or UN sanctions. Indeed, there need not be any US nexus to the transactions at all. Simply engaging in otherwise lawful conduct can result in the imposition of sanctions if the conduct meets specified criteria, resulting not in fines to the offending actors, but in penalties such as being added to OFAC’s List of Specially Designated Nationals and Blocked Persons (‘SDN List’), or severely curtailing access by foreign financial institutions to the US financial system. Inclusion on the SDN List results in the blocking of all property under US jurisdiction, and US persons and businesses are broadly prohibited from transacting with such entities. And, cutting off a foreign bank’s access to the US financial systems can severely reduce its ability to engage in international commercial activity, which is still largely transacted in US dollars.

These are extraordinarily powerful tools and not ones that the US government wields lightly. In August 2017, President Trump signed the Countering America’s Adversaries Through Sanctions Act (Pub. L. No. 115-44) (‘CAATSA’), which provides broad new secondary sanctions authorities to target foreign financial institutions facilitating significant transactions involving Russian energy projects, foreign entities that make significant investments in Russian oil projects, or foreign entities that facilitate significant transactions involving Russian SDNs, among other provisions. Section 231 of that bill also mandated the imposition of secondary sanctions on foreign entities that engage in significant transactions with identified entities in the Russian defence and intelligence sectors, a particular concern for China and Vietnam, which continue to be among Russia’s largest markets for arms exports.

In January 2018, however, the State
Department announced that it would not be imposing sanctions under Section 231 at this time because it had already achieved its intended impact of deterring major new arms deals with Russia. It remains to see how aggressively the Trump Administration will implement CAATSA going forward.

The decision not to aggressively implement CAATSA in the immediate term makes it all the more notable that the Trump Administration has explicitly threatened the use of secondary sanctions in the context of North Korea. Under Executive Order 13810, issued on 25 September 2017, which follows the model used against Iran in the past, OFAC now has the authority to sanction any entity that has engaged in at least one ‘significant’ importation from or exportation to North Korea of any goods, services, or technology, or that has ‘materially assisted’ or ‘provided financial, material, or technological support for, or goods or services to or in support of, any person’ whose property is blocked under the Order, as well as to sanction any foreign financial institution that knowingly conducts or facilitates such transactions in connection with trade with North Korea or involving other sanctioned parties.

That is a model the United States used to great effect in targeting third-country activity with Iran prior to the JCPOA. While that deal resulted in the termination of most secondary sanctions as they applied to transactions with Iran, certain authorities remain in place – namely, OFAC can still sanction third-country firms for engaging in significant transactions with Iranian individuals or entities on the SDN List or with the Islamic Revolutionary Guard Corps (‘IRGC’) and its designated agents and affiliates. Given the IRGC’s vast presence in the Iranian economy, including in the oil and gas sectors where Chinese, Japanese, and Korean firms have made significant investments, secondary sanctions remain a serious risk.

Complicating matters even further, the Trump Administration has threatened to walk away from the JCPOA in May of this year unless perceived deficiencies in the deal are addressed by the P5+1 and Iran. That would likely mean the reinstatement of full US secondary sanctions authorities targeting transactions in Iran’s energy, shipping and shipbuilding, and insurance industries, among others. Such secondary sanctions were frequently threatened but rarely levied by the Obama Administration, as the EU coordinated its own sanctions policies to align more closely with the United States, and Asian countries agreed to reduce their trade with Iran. It is less certain that the Trump Administration would adopt such an incremental approach should it withdraw from the JCPOA, which could result in enormous exposure for Asian firms that continue to do business in Iran.

**The choice being presented to Chinese banks, among others, is stark: they can continue doing or facilitating business involving North Korea or risk losing their access to the United States and US dollar.**

Enforcement trends
The decision to impose secondary sanctions is largely a political question that will depend upon what sort of pressure the US government is trying to exert in any given instance. By contrast, political considerations do not factor heavily in the decision to enforce existing US primary sanctions laws and regulations where there is some nexus with the United States. And here, the trend lines are clear – while there were no OFAC civil enforcement actions brought against Asian companies in either 2015 or 2016, there were four such actions in 2017, including the two largest settlement agreements of the year.

In contrast to the imposition of secondary sanctions, civil or criminal liability for violating US primary sanctions can only arise where there is some US nexus to the transaction allowing the United States to assert jurisdiction. This does not mean, however, that only US individuals or companies can be held liable. Indeed, many of the largest fines in recent years have involved foreign entities that were found liable either because they re-exported US origin goods and services to sanctioned countries or because they ‘caused’ a US person to violate sanctions by using the US dollar in transactions involving sanctioned countries.

Last year’s enforcement actions targeting Asian firms illustrate the risks posed by doing business in or with countries like Iran and North Korea. In July, Singapore-based CSE TransTel Pte. Ltd. agreed to pay $12 million to settle potential civil liability for causing financial institutions to engage in an export or re-export of financial services from the United States to Iran. According to OFAC, CSE TransTel violated Iran sanctions by originating US dollar wire transfers from an account in Singapore to the suppliers for its telecom contracts for energy projects in Iran, thereby ‘causing’ US banks to process transactions involving Iran. And in March, China-based ZTE Corp. agreed to pay $892.3 million as part of a civil and criminal settlement with OFAC, the US Department of Commerce, and the US Department of Justice (‘DOJ’), for illegally re-exporting US origin items to Iran. The action resulted in OFAC’s largest ever settlement with a non-financial entity, and the largest criminal fine ever imposed by DOJ in connection with a sanctions prosecution.
While the CSE TransTel and ZTE Corp. settlements received the most attention, a lower-profile enforcement action might prove more portentous for Asian businesses. In February 2017 OFAC issued a finding of violation to (but imposed no fines upon) B-Whale Corporation ("BWC"), a Taiwanese shipping company that was alleged to have conducted a single ship-to-ship transfer of Iranian-origin crude oil in international waters. There was no allegation that the transaction involved US dollars or the export of US origin products. Rather, OFAC’s basis for asserting jurisdiction was that BWC had entered into bankruptcy proceedings in the Southern District of Texas when the transaction occurred, and thus had voluntarily submitted itself and its property (including its vessels) to US jurisdiction. By receiving Iranian origin crude, then, BWC had engaged in an unlawful importation of Iranian origin goods 'into' the United States, even though neither the vessel nor the crude ever physically entered the country. This seemingly attenuated nexus between the sanctioned transaction and the United States suggests a willingness to use existing primary sanctions authorities aggressively.

Conclusion
OFAC’s expanding authority to impose secondary sanctions, as well as the US government’s aggressive assertions of jurisdiction in sanctions enforcement actions, pose a significant risk for East and Southeast Asian companies that may be facilitating business with North Korea or expanding their otherwise lawful trade with Iran or Russia. Because US sanctions on North Korea only intensified in 2016 and it can take several years for enforcement actions to develop, new civil and criminal penalties against firms in East and Southeast Asia are almost certain to emerge. Similarly, the Trump Administration’s waning patience in addressing either the North Korea or Iran issues through diplomatic efforts suggests that the aggressive imposition of secondary sanctions may be forthcoming.

It is critical, then, that East and Southeast Asian companies rigorously assess their potential liability under US law and their potential exposure to US sanctions, especially if they are engaged in or facilitating significant transactions with sanctioned countries. This should include an investment in compliance, to include an inquiry into all potential US touchpoints to a transaction as well as due diligence into the identity and business profile of any intermediaries, distributors, or counterparties. Given the considerable discretion the US government has afforded itself in this arena, it also means a critical assessment of whether the risks might outweigh the benefits when doing business involving countries like Iran and North Korea.

Sean Kane is counsel in the Washington, D.C., office of Hughes Hubbard & Reed LLP. He was formerly the Deputy Assistant Director for Policy at the Office of Foreign Assets Control.

sean.kane@hugheshubbard.com

Enter the global market.

Achieve end-to-end visibility and operational efficiency in your global supply chain.

INCREASE PRODUCT INNOVATION | MITIGATE COMPLIANCE RISKS | IMPROVE TIME-TO-MARKET

For more information, please visit www.AmberRoad.com

29 WorldECR www.worldecr.com
CSE sanctions breaches: the long arm of US sanctions

In 2017, Singapore’s CSE agreed a USD 12 million settlement with OFAC – not for breach of US sanctions itself but for having caused US financial institutions to breach them. Karnan Thirupathy and Elizabeth Fong review the case and its implications for non-US companies.

Last year, the Singapore listed company CSE Global Limited (‘CSE Global’) and its wholly-owned Singaporean subsidiary CSE TransTel Pte. Ltd. (‘CSE TransTel’) (collectively referred to as ‘CSE’) entered into a settlement agreement with the US Department of the Treasury’s Office of Foreign Assets Control (‘OFAC’) requiring CSE to pay a settlement of USD 12 million. This penalty was imposed on CSE in response to its apparent violations of US sanctions by using US dollar accounts with its Singapore bank to make payments to various entities in relation to Iran-related contracts.

The action taken by OFAC is significant in that it appears to be an indication that the US is now actively enforcing sanctions more broadly, even against non-US, non-financial companies operating outside the US. The case also illustrates how the use of USD in transactions may expose non-US entities to the risk of running afoul of US sanctions regulations.

Dealing with sanctioned entities
From around June 2012 to March 2013, CSE TransTel had apparently violated the International Emergency Economic Powers Act (the ‘IEEPA’) and the Iranian Transactions and Sanctions Regulations (the ‘ITSR’) by its dealings with Iranian entities through an Iranian subsidiary, TransTel Engineering Kish Co Ltd.

Specifically, CSE TransTel had:

- Entered into contracts with, and received purchase orders from, multiple Iranian companies to deliver and install telecommunications equipment for the South Pars Gas Field in the Persian Gulf, the South Pars Power Plant in Assalouyeh, Iran, and the Reshadat Oil Field in the Persian Gulf between 25 August 2010 and 5 November 2011.
- Hired and engaged various third-party vendors – including several Iranian companies – to provide goods and services on its behalf in connection with the contracts and purchase orders set out above.

The Iranian entities which CSE TransTel had conducted business with included Petropars, which OFAC had identified as a sanctioned entity owned or controlled by the government of Iran, and the Iran Maritime Industrial Company SADRA, which was an entity on OFAC’s Specially Designated Nationals and Blocked Persons (‘SDN’) List.

Causing US financial institutions to breach sanctions regulations
CSE Global and CSE TransTel had maintained separate USD and Singaporean Dollar (‘SGD’) accounts with a non-US financial institution in Singapore (the ‘Bank’). Prior to entering into the various transactions with Iranian entities, CSE had given an undertaking, signed by CSE TransTel’s Managing Director and CSE Global’s Group CEO, ‘not to route any transactions related to Iran through the Bank, whether in Singapore or elsewhere.’

However, within two months of executing this undertaking, CSE TransTel breached it by making USD transfers from its USD-denominated account with the Bank relating to its Iranian business. The relevant transactions were processed through multiple financial institutions, including US financial institutions, to engage in the exportation or re-exportation of financial services from the United States to Iran, which is an activity prohibited under the IEEPA and the ITSR.

The case illustrates how the use of USD in transactions may expose non-US entities to the risk of running afoul of US sanctions regulations.

The case also illustrates how the use of USD in transactions may expose non-US companies operating outside the US to the risk of running afoul of US sanctions regulations.

Settlement agreement
OFAC found CSE TransTel’s violations of its sanctions regulations to be egregious in nature, given the extent of the violations and the fact that CSE TransTel had failed to make any voluntary self-disclosures of these violations despite having ample opportunity to do so at any time.

As such, if CSE TransTel had disputed the charges, OFAC would have claimed the maximum civil monetary penalty that could have been levied against them, which in this case, totalled USD 38,181,161.

While CSE TransTel had maintained that the funds transfers were payments for non-US goods and services,
services which were lawfully provided by CSR TransTel to Iran or Iranian entities via non-US third-party vendors, CSE Global released a statement setting out that CSE would settle the matter with OFAC. This is understood to be mainly because CSE noted that the alternative to settling would entail ‘costly and lengthy litigation in the US’, which would require CSE to dedicate a great deal of time and resources towards an uncertain outcome.

The net result was that CSE agreed, amongst other things, to agree to pay a sum of USD 12,027,066 to the US Department of the Treasury in settlement.

The significance of the CSE settlement
The CSE settlement has far-reaching implications and is significant in a number of respects. Four of the more immediately obvious implications are discussed below:

1. OFAC is extending its reach
This is apparently the first time that OFAC has used its statutory authority to target a non-US, non-financial institution which had caused US financial institutions to process USD transactions involving a sanctioned jurisdiction. It appears that the US is becoming increasingly willing to extend its reach.

It is possible that the CSE settlement is an indication that the Trump administration may be taking a harder stance against sanctioned states such as Iran. Whilst President Trump has recently indicated that the US would ‘waive’ oil and banking sanctions against Iran until May 2018, he has indicated that this may be the last time that the US will agree to such ‘waivers’. The stance taken is of course not entirely surprising given that President Trump had consistently described the Joint Comprehensive Plan of Action, which was struck between Iran and the P5+1 (China, France, Russia, the United Kingdom, and the United States; plus Germany) as the ‘worst deal ever’.

2. Non-US entities transacting in USD may be affected by US sanctions regulations
While OFAC has stated that the use of USD in itself does not create a jurisdictional nexus, all wire transfers in USD are routed through the US and its financial systems, and would necessarily involve US financial institutions. This case highlights how the making of USD payments could potentially cause a non-US company operating outside the US to be in breach of OFAC’s sanctions regulations due to the involvement of US financial institutions, even where the company is dealing with a non-US bank.

Companies should pay extra attention to sanctions compliance issues when originating USD transfers where the underlying transaction may involve countries or entities that may be subject to US sanctions. This case illustrates that even a non-US company operating outside the US can easily be in breach of US sanctions by causing US financial institutions to ‘engage in the exportation or re-exportation of financial services from the United States to Iran’. It is not unknown (or surprising) that some non-US companies operating outside the US choose to transact in other (non-USD) denominations such as the Euro or Renminbi where possible to minimise the involvement of US financial institutions and accordingly to minimise the risk of US sanctions being breached.

Although the current action was brought against a company that made payments in USD, going forward, OFAC could also seek to enforce US sanctions in situations where non-US companies receive USD payments involving OFAC-sanctioned jurisdictions and parties. It would therefore be prudent for non-US companies to take a cautious approach where any payments are being made or received in USD – even if the transaction does not otherwise involve any US entities.

3. OFAC may also levy criminal penalties on violators of its sanctions regulations
Apart from OFAC’s ability to impose civil monetary penalties, entities originating funds transfers in USD involving OFAC-sanctioned jurisdictions or parties may also potentially be subject to criminal liability. Depending on the facts of the case, the US authorities may proceed on either civil or criminal actions, or even both.

4. Companies must adhere to undertakings which they provide
A feature of this case, which in our experience is becoming increasingly common, is that the company had given an express written undertaking to its bank that it would not route any transactions to Iran through the bank.

A company providing such undertakings to its bank must take the undertakings seriously and should have internal compliance procedures in place to ensure that the undertakings are adhered to. The breach of the undertaking by CSE in the present case, may have made CSE’s conduct appear more culpable in that they could be taken as an indication that CSE had negligently (or intentionally) misled its bank or concealed the fact that CSE was conducting potentially sanctioned business through the bank.

Financial institutions will not consider the provision of such undertakings to be a mere box-checking exercise when setting up accounts. Banks are well aware of the risks of possible sanctions breaches, and obtaining such undertakings from customers are part of their own sanctions compliance and risk mitigation procedures. As the present case illustrates, if the transaction turns out to be in breach of sanctions, the banks will rely on the undertaking given by the customer and OFAC will take the undertaking into consideration as a factor when determining the company’s culpability and the level of penalty to impose.

The wording of the undertakings requested by banks do vary. If a company is not confident that it will be able to comply with the terms of an undertaking required by its bank, the company does generally have the right to negotiate the terms so that they are not overly onerous.

Karnan Thirupathy is a partner and Elizabeth Fong is a solicitor at Kennedys Legal Solutions in Singapore.

karnan.thirupathy@kennedyslaw.com
elizabeth.fong@kennedyslaw.com
Peru: Dual-use export controls in transit and transhipment

The new book from the publishers of WorldECR is Dual-Use Export Controls in International Transit and Transhipment. In this extract, Julio Guadalupe introduces the export controls regime of South American country, Peru. The book features more than 40 country chapters covering the Americas, EMEA and Asia Pacific.

Peru does not specifically regulate dual-use goods. The rules for customs transit and transhipment are governed by the general provisions that are set forth in the General Customs Law (Ley General de Aduanas). However, Peruvian regulations on customs controls are generally consistent with the provisions of the Kyoto Convention (as amended), as well as the various free trade agreements signed by Peru that address customs procedures and the facilitation of trade.

Legal framework
The following laws and regulations form the legal basis for transit and transhipment controls in Peru:

- General Customs Law, approved by Legislative Decree 1053, published on 27/6/2008 (as amended).
- General Customs Law Regulations, approved by Supreme Decree 010-2009-EF, published on 16/1/2009 (as amended).
- Schedule of penalties applicable to infractions set forth in the General Customs Law, approved by Supreme Decree 031-2009-EF, published on 11/2/2009 (as amended).
- Kyoto Convention (as amended).
- Legislative Decree 1126 (regulations on chemical supplies and controlled substances).
- Southern Cone International Land Transport Agreement (‘ATIT”).
- Andean Community Decision 502.

Competent agency
Customs is in charge of the management, collection, control and monitoring of international traffic of goods, means of transportation and persons within Peruvian territory. The General Customs Law defines customs administration under the Peruvian National Tax Administration Agency (‘SUNAT’) as the authority responsible for applying customs regulations, collecting customs duties and other taxes applicable to the importation of goods, applying other laws and regulations related to customs operations, and exercising its customs authority and control over goods entering and leaving the country.

Transit
Transit is defined as operations in which goods arriving from abroad, but with a foreign destination, are not assigned to a particular customs category and are transported under customs control from one customs office to another. Such goods are not subject to payment of taxes against provision of a bank guarantee letter.

The transit procedure for goods starts at a customs office of departure, subject to the applicable controls at border customs offices of transit, and concludes at the declared customs office of destination.

Highways connect the territories and capitals of Andean Community member states, and are the backbone of international transportation and customs transit of goods in the Andean sub-region.

There are three types of customs transit procedures: internal customs transit, customs transit to free trade zones and customs transit with a foreign destination.

Goods transiting with a foreign destination must be in closed and properly sealed containers or in a closed and sealed freight car or cars. Self-transported goods must obtain authorisation from the Ministry of Transportation and Communications. All other transiting goods must be
traceable, i.e., identified and individualised.

The office of departure will perform a physical inspection of goods:

- where the dimensions of the goods do not allow them to be shipped in a closed container, provided that the goods are properly identified and individualised;
- where containers are in a poor condition, have weight discrepancies or the seals show signs of having been tampered with;
- or as may be determined by customs authorities.

In addition, the designated customs official performs the external inspection of the condition of the in-transit containers or of the goods to verify that:

- tamper-evident seals are in good condition and do not show signs of tampering or breakage, and are in accordance with the customs declaration (‘CD’);
- the gross weight received at the border control office or temporary warehouse and/or point of entry does not differ from the weight appearing on the CD;
- identification marks, as well as safety measures, are consistent with those used by the entry office, where applicable; and
- the goods have arrived via the means of transportation and within the time period authorised by the office of entry into the country.

Where goods have been destroyed, the filer shall submit documents evidencing their destruction to the customs office with jurisdiction in the territory in which the events occurred. If the goods are partially destroyed, the customs office with jurisdiction shall inform the office of entry in order for it to authorise continuation of transit of the goods.

Where the goods have been totally destroyed, the customs office with jurisdiction shall inform the office of entry.

The following steps are required to process transit goods through customs:

- The filer shall submit a bank guarantee letter equal to the FOB value of the goods.
- The transportation company must be authorised to operate by the competent authorities; i.e., the Ministry of Transportation and Communications (‘MTC’).
- The transit information must be contained in the CD and the CD must be submitted to customs officials.
- Officials will review CD forms and documents.
- There is a physical inspection of the goods.
- The goods are released or withdrawn from the point of entry at the customs office of arrival.
- The goods are received at a customs office in the country or at the customs office of departure in free trade zones.
- Entry of recorded goods to a temporary warehouse and/or point of arrival at a customs office in the country, the customs office of departure or to a free trade zone.
- The operation is formally concluded.
- The bank guarantee letter is refunded.

The following goods are restricted from transit:

- Firearms and explosives.
- Nuclear waste or toxic waste.
- Precursor products for manufacturing narcotics or drugs not authorised by the Ministry of Health.
- Goods for which there are legal or administrative restrictions on performing this type of operation.
- Goods transported by means of transportation, or contained in cargo units that cannot be properly tamper-proof sealed.

Transhipment

Transhipment is where goods are unloaded from the means of transportation used for arrival in the customs territory and then loaded onto a means of transportation used to depart the customs territory, under the control of the customs authority.

Transhipment may simply be direct or goods might be unloaded to the dock or a customs warehouse. The transhipment of goods is at the request of the transportation company and is accompanied by the cargo manifest using the specified customs transhipment declaration form.
containing information on the cargo under transhipment.

Goods under transhipment will not be physically inspected except where packaging is in poor condition; containers show signs that their safety seals have been tampered with; or at the request of the customs authority.

The customs procedure for transhipped goods are as follows:

i. The filer submits the information contained in the customs declaration for the goods online using the specified customs transhipment declaration form.

ii. The customs computer system – the Sistema Informático de la Aduana, or ‘SIA’ – processes the submitted information, and if in order, automatically generates a customs declaration number. Otherwise, the reason for the rejection is indicated.

iii. Once a number has been assigned to the declaration, the SIA validates the submitted cargo manifest, the customs transhipment declaration and the transportation document for said goods. The SIA then automatically authorises the customs transhipment operation for a period of thirty (30) calendar days as of the numbering of the customs transhipment declaration and records said information.

Violations and penalties

Article 192 of the General Customs Law stipulates that violations punishable with fines are committed by ‘[f]oreign traders, in case of: failure to comply with the time limits established by customs authorities for reshipment, customs transit, transhipment of goods, onboard supplies …’. Fines in these cases can amount to approximately US$1,200 and the goods may be confiscated.

Chemical supplies and controlled substances

Legislative Decree 1126 enacted regulations for customs control of chemical supplies and controlled substances (‘CSCS’) that can be directly or indirectly used to manufacture illegal drugs.

In accordance with these regulations, in order for CSCS to enter the country they must have control records and be authorised for legal entry and exit from national territory.

Notwithstanding the foregoing, pursuant to Article 38 of the Regulations for Legislative Decree 1126 (Supreme Decree 044-2013-EF), the above authorisation shall not be required for CSCS operations involving international transit, transhipment and reshipment. Although not expressly indicated by the regulations, in these cases, CSCS control records are also not required.

For CSCS operations involving customs transit within national territory, the SUNAT, assisted by the national police, shall carry out the control of said goods while they are in Peruvian territory, and is authorised (among others) to:

i. request from the carrier the international cargo manifest and customs transit declaration (MIC/DTA), international cargo manifest and international customs transit declaration (MIC/DTAI), customs declaration or equivalent documentation duly authorised or legalised by the customs authority;

ii. verify the condition of the security devices indicated in the submitted documentation, and SUNAT is authorised to open the containers holding the transported controlled goods;

iii. use electronic devices to monitor the vehicle while it is in national territory; and

iv. monitor the use of mandatory transportation routes for controlled goods.

Integrated border customs control

Andean Community Decision 502 created bi-national border control centres that provide integrated customs control operations between Andean Community member states (Bolivia, Colombia, Ecuador and Peru) in an effort to reduce processing times for customs transit and clearance operations. It also seeks to increase the flow of cargo movement, increase transparency of foreign trade operations, facilitate the exchange of import and export information and prevent smuggling.

Accordingly, the integrated control activities include:

- Correlated numbering of entry and/or exit cargo manifests.
- Online operations records.
- Cargo manifests inspected by both customs offices.
- Daily information sharing (signed reports).
- Periodic information exchange records.
- Integrated control committee records.
- Integrated control operations guidelines.

Conclusion

Peru does not have specific regulations for customs transit and transhipment of dual-use goods but they are governed by the general provisions set forth in the General Customs Law. Strict controls are in place for the transit of goods, requiring integrated control (physical inspection and inspection of the condition of containers) between the customs offices of arrival and departure from the country or a free trade zone.

With respect to the transhipment of goods, regulations provide for controls carried out in the primary zone regarding movement of goods from one means of transportation to another. This type of control involves computer validation by customs of the information provided by the carrier.

Peru is also a signatory to agreements within the framework of ALADI, the Andean Community (‘AC’) and other countries in South America, allowing for the integrated control of operations along the borders of these countries and facilitating processing and management of risk related to international transit of goods.

Julio Guadalupe is a partner of Rodrigo, Elias & Medrano Abogados in Lima.

www.estudiorodrigo.com
Dual-Use Export Controls in International Transit and Transhipment

Dual-Use Export Controls in International Transit and Transhipment is the newly released book from the publishers of WorldECR, the journal of export controls and sanctions.

The book updates a report WorldECR originally published in 2012 on the transit and transshipment regimes of countries in the Americas, Europe, Asia and the Middle East. At the urging of many of our readers, we have now re-published in hard copy, providing up-to-date coverage and including a much larger number of jurisdictions than contained in the original report.

Dual-Use Export Controls in International Transit and Transhipment reflects the growing complexity and regulation involved in the transport of freight, not only between differing jurisdictions but also within individual jurisdictions themselves. Each point in the freight journey may give rise to issues that impact, for example, a cargo’s licensing and customs inspection, a process that could in turn have consequences not only for costs but the ultimate success of any freight transaction.

In keeping with the remit of WorldECR, the main focus is on transit and transshipment laws as they apply to dual-use goods. However, as is evidenced in the book’s country-by-country analysis, a significant number of jurisdictions have no established regime aimed at regulating dual-use versus other types of goods, leaving the transit and transshipment of freight subject to an often-complex array of local customs laws.

The book also examines the different regulations as they may pertain to the types of carriage. Writing in the Foreword, WorldECR editor, Tom Blass, notes that while the terms ‘transit’ and ‘transhipment’ are frequently used in close proximity to each other, they should not be used interchangeably: ‘A pallet of widgets originating in France is in transit as it travels through Belgium on the back of a truck, but is transhipped on being unloaded from the truck in Hamburg and placed aboard a ship bound for the United States.’

Chapter by chapter
Each chapter is written by an expert in export controls in his/her jurisdiction. Chapter authors detail the export control regime/framework in their country, explaining how transit and transshipment are locally defined and controlled and how controlling regulations are enforced. Useful information on competent authorities, procedures, and penalties for breach is included in most country chapters along with contact details for licensing authorities. Information on free trade and special economic zones is included for some countries.

How to order
Dual-Use Export Export Controls in International Transit and Transhipment is available from directly from WorldECR. Copies cost £85 (plus postage and packing). For further information and to order your copy, please email info@worldecr.com with your order requirements. Discounts for bulk orders are available (email for details).

Chapters and contributing authors

The Americas: Argentina by L. Augusto Vechio; Brazil by Alessandra Machado and Marcelle Silbiger; Canada by Wendy Wagner; Chile by Gaston Medina; Colombia by César Camilo Cermelo; Mexico by Horacio A. López-Portillo; Peru by Julio Guadalupe; USA by Tamer Soliman, Jing Zhang and Bernd Janzen

Europe and the EU: Albania by Besnik Duraj and Bojana Hajdini; Belgium by Fabienne Vermeeren and Charlotte Van Haute; Cyprus by Elena Christodoulou; Denmark by Anders Hedetof and Anna Martine Stubben; France by Diederik Cops and Nils Duquet; Germany by Dr. Bärbel Sachs; Greece by Michalis Kosmopoulos and Mariliza Kyparissi; Italy by Silvia Salmaso; Netherlands by Jikke Biermasz and Petra Chao; Norway by Hugo Munthe-Kaas and Pernille Engstrøm Skaug; Poland by Krzysztof Korwin-Kossakowski and Kuba Ruiz; Portugal by Tiago Marreiros Moreira and Catarina Belim; Romania by Adrian Roseti and Claudia Hutina; Spain by Diego Pol and Valeria Enrich; Sweden by Mattias Hedwall; Switzerland by Peter Henschel and Prof. Dr. Andreas Furrer; Ukraine by Gleb Bialyi and Oleksandr Maydanyk; United Kingdom by Rhys Williams

Asia and the Middle East: Australia by David Howard and Alexandra Shearer; China by Bo Xue; Egypt by Yulia V. Akinfiev; Hong Kong by George Tan and Cecil Leong; India by Sanjay Notani and Rohit Jain; Iran by Ali Pirmoradi and Zahra Darvish; Israel by Gil Rosen; Japan by Tamotsu Aoi; Malaysia by Cynthia Lian; Singapore by George Tan; South Korea by Jae Won Lee; Turkey by S. Mustafa Durakoğlu; United Arab Emirates by Ryan Cathie.
The missile sanctions gap: realigning US and EU Iran designations

January 2018 brought with it two key recurring deadlines for US President Donald Trump: whether or not to certify Iran’s compliance with the JCPOA nuclear deal and whether to continue waiving nuclear-related sanctions on Iran. On 12 January, President Trump decided for a second time not to certify Iran’s compliance, but he stopped short of re-imposing sanctions. Instead, he waived sanctions once again to allow time to ‘fix the deal’s disastrous flaws,’ including by securing Europe’s cooperation in addressing Iran’s ballistic missile threat. The president warned, however, that this would be ‘a last chance’ and that without progress he would ‘withdraw from the deal immediately.’ Such progress could begin with a return to greater coordination between the US and EU on missile-related designations against Iran.

The sanctions coordination gap

The 12 January sanctions waivers were accompanied by another round of US Treasury Department sanctions, including against entities supporting Iran’s military-related procurement. Earlier in January, the Treasury Department designated five entities for their support of Iran’s solid fuel ballistic missile programme. These are the latest in a string of actions by the United States against Iranian missile proliferators, which have been taken in conjunction with sanctions targeting the Iranian government’s support for terrorism, human rights abuses, and its destabilising regional actions.

By contrast, the European Union has not sanctioned any Iran-related entities of proliferation concern since 22 December 2012. While neither the US nor the EU designated any entities during the height of the nuclear negotiations in 2015, the US resumed such designations in January 2016 – just one day after the implementation of the JCPOA. Since the JCPOA’s implementation, the US has designated 73 proliferation-related entities, only three of which appear on the EU list. The majority of these entities are derivative designations targeting subsidiaries and overseas networks of suppliers, front companies, and individuals acting on behalf of already designated entities. Most were targeted for supporting Iran’s ballistic missile programme, with a fewer number designated for supporting Iran’s military, including through illicit procurement.

In his 12 January statement, President Trump called on Europe to join the US in taking ‘stronger steps’ aimed at ‘constraining Iran’s missile development and stopping the proliferation of missiles, especially to Yemen.’ He also described ongoing efforts to work with European allies on ‘a new supplemental agreement that would impose new multilateral sanctions if Iran develops or tests long-range missiles.’

Congress, too, has called for greater cooperation between the US and the EU in efforts to constrain Iran’s missile development, including by coordinat- ing proliferation designations. Such coordination was one reason for the high impact of international sanctions in the period before the 2015 nuclear agreement. The Countering America’s Adversaries Through Sanctions Act (CAATSA, P.L. 115-44), which President Trump signed into law last August, requires the administration to report to Congress every 180 days on the discrepancies between US and EU WMD or missile proliferation sanctions. The first such report was due at the end of January.

While a number of EU Member States agree on the need to confront Iran’s missile programme, EU foreign affairs chief Federica Mogherini repeatedly has emphasised the need to address ballistic missiles outside of the nuclear agreement.

The reluctance of the EU to coordinate with the US on non-nuclear sanctions against Iran post-JCPOA undermines US sanctions and efforts to stem Iran’s missile programme, argue Valerie Lincy, Mana Mostatabi, and Meghan Peri Crimmins.
Council resolution 2231.10 to UN sanctions pursuant to Security of the 73 entities designated by the US decisions and regulations since 2007. Like the US executive order, these authorities provide that the sanctions – including an asset freeze and prohibition on transactions – apply to those entities acting on behalf of, or owned or controlled by, those that are explicitly designated. However, the EU has failed to take action against such related entities since the nuclear agreement’s implementation. This makes it easier for Iran’s missile supply network to continue operating and undermines the impact of US sanctions.

**SHIG and SBIG: key to Iran’s ballistic missile programme**

SHIG is responsible for Iran’s liquid-fuelled ballistic missile programme and has engaged in the transfer of controlled missile technology with North Korea. SBIG is responsible for Iran’s solid-fuelled ballistic missile programme and produces Iran’s Fateh-100 short-range missile. Twenty-eight of the 73 entities designated by the US are subordinates or suppliers to SHIG or SBIG, both of which remain subject to UN sanctions pursuant to Security Council resolution 2231.

The US focus on SBIG and SHIG increased after Iranian-backed Houthi militants in Yemen launched short-range ballistic missiles into Saudi Arabia on three occasions between July and December 2017. SBIG’s logo and SHIG’s name were found imprinted on missile parts recovered from two of the missile strikes. A UN investigative panel for Yemen reportedly stated that, by failing to prevent the Houthis from acquiring the missiles, Iran may be in ‘noncompliance’ with Security Council resolution 2216, which imposes a targeted arms embargo on Yemen.

The US has continued to target subsidiaries of SHIG and SBIG, most recently on 4 January, when the Treasury Department designated five entities for their role in developing and producing missile guidance systems, propellant for solid-fuelled ballistic missiles, and ballistic missile launchers. All five are ‘owned or controlled’ by SBIG.

US sanctions also have aimed to shut down the overseas supply networks used by SHIG and SBIG. For example, in February 2017 the Treasury Department designated a key Iranian procurement agent, Abdollah Asgharzadeh, and a network of China-based brokers and companies used by Asgharzadeh to procure dual-use technology for SHIG. The Asgharzadeh network procured and shipped foreign-produced ball bearings required for the Shahab-2 and Shahab-3 ballistic missiles. Also in February 2017, the Treasury Department targeted a Dubai-based procurement network supplying SBIG with ballistic missile components.

**SEI: targeting proliferation abroad**

SEI produces electronic equipment for the Iranian military, including radars, avionics and control systems, and missile guidance technology. The firm has used front companies and individuals globally to obtain sensitive US-origin missile-related goods and technology.

Half of the 28 foreign firms sanctioned by the United States for proliferation since the JCPOA’s implementation were targeted for their support of SEI or its parent, IEI. For example, in July 2017, the Treasury Department designated a China-based procurement agent and a network of Chinese companies she used to procure US-, Canadian-, and European-origin electronic components on behalf of SEI. In May 2017, the Treasury Department designated another Chinese national and three associated China-based companies for supplying SEI with goods and technology used for missile navigation, guidance, and stabilisation. Some transactions have taken place ‘since at least 2015,’ the year of the nuclear agreement.

In the Treasury Department’s most recent action on 12 January, yet another China-based supply network was sanctioned for selling specialised sensors and navigational gyrocompasses to SEI. SEI and IEI also have been connected to military-related exports to Yemen. In January 2016, a UN investigative panel concluded that weapons seized by the US and Australia while en route to Yemen were likely of Iranian origin. The panel’s report noted that the weapons bore ‘the markings bearing the names of Iranian industrial companies’ and contained photos revealing stamps belonging to SEI and IEI.

**The European Union faces several challenges in pursuing designations that would realign its sanctions with those of the United States.**

The European Union faces several challenges in pursuing designations that would realign its sanctions with those of the United States. First, establishing consensus among the EU’s 28 Member States is difficult. France has taken a firm stance, calling Iran’s missile programme ‘inconsistent’ with UN resolutions and ‘a destabilizing factor in the region.’ In a speech on 8 January, French President Emmanuel Macron noted that Iran’s ‘ballistic missile activity has been stepped up’ since the 2015 nuclear agreement, and that dialogue with Iran to restrict this activity is ‘essential.’ Other countries, however, have been less forceful in calling for action.

Second, the EU is concerned that any punitive action against Iran’s missile programme could further undermine the nuclear agreement, which they judge as already in jeopardy as a result of the US administration’s actions. In remarks last November, Mogherini said that the EU was ‘ready to addresses other issues,’ including missiles, ‘once it is very clear that the nuclear deal implementation is preserved by all sides [in] full.’

Finally, the EU has faced legal
challenges to its designations in recent years. Some Iranian companies and individuals have disputed their designation in EU courts and have had sanctions against them lifted because the information used to support the designation was confidential. Such information could not be shared openly in court and with the defendants. This may have increased the evidentiary burden required for the EU to issue additional autonomous designations, including derivative designations against subordinates and suppliers of sanctioned entities.

A way forward

Recent statements by US and EU officials indicate a desire to work together to address the threats posed by Iran that the nuclear agreement did not contain including Iran’s ballistic missile programme. During a recent visit to London, US Secretary of State Rex Tillerson announced that a working group had been set up with France, Germany, and the United Kingdom to discuss these threats and ‘how we might approach Iran to address our concerns’.23

In addition, French Foreign Minister Jean-Yves Le Drian will be travelling to Iran in early March to discuss Iran’s missile programme along with related ‘regional questions’.24 He promised to deliver a ‘frank message’ about the need for Iran to contain its missile programme as required by Resolution 2231.25 Finally, Germany reportedly advocating for targeted EU economic sanctions aimed at punishing Iran’s missile programme.26 If Iran refuses to curb its missile development through negotiations, a package of such sanctions reportedly be adopted.27 These are welcome developments. Closer collaboration between the United States and Europe increases the prospect of meaningfully restricting Iran’s missile work whether through negotiation, economic pressure, or both.

---

Valerie Lincy is executive director, Maria Mostatabi is a research associate and Meghan Peri Crimmins is a senior associate at the Wisconsin Project on Nuclear Arms Control.

[www.wisconsinproject.org]

---

6 ‘Some Iranian Companies and Individuals have disputed their Designation in EU Courts and have had Sanctions against them Lifted because the Information used to Support the Designation was Confidential. Such Information could not be Shared Openly in Court and with the Defendants. This may have increased the Evidentiary Burden Required for the EU to Issue Additional Autonomous Designations, Including Derivative Designations against Subordinates and Suppliers of Sanctioned Entities.’
7 ‘A Way Forward,’ Recent Statements by US and EU Officials Indicate a Desire to Work Together to Address the Threats Posed by Iran that the Nuclear Agreement did Not Contain Including Iran’s Ballistic Missile Programme. During a Recent Visit to London, US Secretary of State Rex Tillerson Announced that a Working Group had Been Set Up with France, Germany, and the United Kingdom to Discuss These Threats and ‘How We Might Approach Iran to Address Our Concerns.’ In Addition, French Foreign Minister Jean-Yves Le Drian will be Travelling to Iran in Early March to Discuss Iran’s Missile Programme along with Related ‘Regional Questions.’ He Promised to Deliver a ‘Frank Message’ about the Need for Iran to Contain its Missile Programme as Required by Resolution 2231. Finally, Germany Reportedly Advocating for Targeted EU Economic Sanctions Aimed at Punishing Iran’s Missile Programme. If Iran Refuses to Curb its Missile Development through Negotiations, a Package of such Sanctions reportedly be Adopted. These are Welcome Developments. Closer Collaboration between the United States and Europe Increases the Prospect of Meaningfully Restricting Iran’s Missile Work whether through Negotiation, Economic Pressure, or Both.

---

Links and notes

6 ‘Some Iranian Companies and Individuals have disputed their Designation in EU Courts and have had Sanctions against them Lifted because the Information used to Support the Designation was Confidential. Such Information could not be Shared Openly in Court and with the Defendants. This may have increased the Evidentiary Burden Required for the EU to Issue Additional Autonomous Designations, Including Derivative Designations against Subordinates and Suppliers of Sanctioned Entities.’
7 ‘A Way Forward,’ Recent Statements by US and EU Officials Indicate a Desire to Work Together to Address the Threats Posed by Iran that the Nuclear Agreement did Not Contain Including Iran’s Ballistic Missile Programme. During a Recent Visit to London, US Secretary of State Rex Tillerson Announced that a Working Group had Been Set Up with France, Germany, and the United Kingdom to Discuss These Threats and ‘How We Might Approach Iran to Address Our Concerns.’ In Addition, French Foreign Minister Jean-Yves Le Drian will be Travelling to Iran in Early March to Discuss Iran’s Missile Programme along with Related ‘Regional Questions.’ He Promised to Deliver a ‘Frank Message’ about the Need for Iran to Contain its Missile Programme as Required by Resolution 2231. Finally, Germany Reportedly Advocating for Targeted EU Economic Sanctions Aimed at Punishing Iran’s Missile Programme. If Iran Refuses to Curb its Missile Development through Negotiations, a Package of such Sanctions reportedly be Adopted. These are Welcome Developments. Closer Collaboration between the United States and Europe Increases the Prospect of Meaningfully Restricting Iran’s Missile Work whether through Negotiation, Economic Pressure, or Both.

---

Valerie Lincy is executive director, Maria Mostatabi is a research associate and Meghan Peri Crimmins is a senior associate at the Wisconsin Project on Nuclear Arms Control.

[www.wisconsinproject.org]
Smart contracts, blockchain and export control compliance

The years 2016 and 2017 were dominated by the hype of Bitcoins and the large amount of capital raised via blockchain technology in initial coin offerings (ICOs), also known as token sales or token generation events (TGEs). While public discussions focus mainly on Bitcoin and ‘cryptocurrencies’, the compliance community responsible for export controls should take a closer look at the real potential of blockchain technology in business process digitisation and the important role of compliance officers in such blockchain projects. This article will give a high-level overview of the impact of blockchain-enabled business processes on the role of compliance managers and officers.

Blockchain beyond Bitcoin: impact on international trade

More and more established businesses are now considering blockchain technology (also known as distributed and decentralised ledger technology, or ‘DLT’) to improve their business processes. Blockchain technology uses cryptography, a type of random computer-generated and unbreakable code, to ensure that transactions remain private and secure. Enterprises should consider this technology to safeguard the integrity of business processes or to store data in a manner that cannot be changed, stolen or otherwise compromised by malicious software or third parties.

Another key benefit of DLT in the context of compliance management is the opportunity to automatically perform complex business processes and contractual commitments via smart contracts, a software that defines a set of orders in computer code and automatically enforces those obligations, triggered by external data sources (so-called ‘oracles’).

To illustrate how smart contracts can apply in the context of international trade and compliance management, imagine that a ship arrives into port, after which the container is discharged and carried to the buyer’s warehouse. The parties agree that the first portion of the payment from buyer to seller is automatically triggered when the ship arrives at port (e.g., via GPS information), and the payment of the second portion when the goods are delivered, timely and undamaged, at the warehouse (scan and goods-in check by the officer at the ramp of the warehouse). In this case, the payment between buyer and seller is realised peer to peer via a smart contract system. The smart contract transacts the blockchain-based payment of goods after being triggered by oracles (GPS data and goods-in scan info). In such smart contract-based letter of credit systems, the need for trustees as intermediaries (insurances/banks) can be eliminated.

Currently, blockchain protocols such as Ethereum provide the ability to deploy such smart contracts in a secure and transparent way. The setup of these smart contracts allows a high degree of integration and automation, which may render intra-company interfaces and communications obsolete, or at the very least greatly minimised. These smart contracts will be increasingly triggered by blockchain-enabled smart devices (Internet of Things applications serving as oracles) and potentially controlled by artificial intelligence without any human interaction. We are looking at a future where integrated hardware and software will allow any inter-company transactions to be fully digitised and automated, running on decentralised blockchain systems. However, certain legal and compliance boundaries will continue to exist in automated decentralised transactions.

Legal transactions via smart contracts

While blockchain technology advances, many new and innovative business solutions and applications are being developed. At the same time, regulators around the world are increasing their efforts to qualify the new blockchain elements, such as smart contracts,
Blockchaintransacting illegally. Blockchain technology and the ability to automate business processes on the blockchain will allow compliance officers to integrate rules and checks into the smart contract code, such as sanction screening or licence checks. Having all transactions securely recorded on the blockchain will allow compliance officers to easily perform post-transaction auditing. Even more, in a blockchain ecosystem with identified parties and availability of relevant data, such as end-user information, classification and licensing, the task of a compliance officer may become predominantly a role of process and smart contract design.

Compliance functions in a smart contract system
Sanctions and embargo checks will continue to become a standard compliance function within smart contract systems. KYC (here defined as ‘Know your Counterparty’) processes are already used by many blockchain projects, in particular those dealing with the exchange of cryptocurrencies and fiat currency (the latter being recognised by governments as legal tender). The ‘on-ramping’ of blockchain users (i.e., receiving cryptocurrencies in exchange for fiat), or the ‘off-ramping’ from cryptocurrencies back to fiat, requires blockchain-based exchange operators to establish relevant KYC processes, which aim to identify individuals or entities that may be sanctioned or may represent an elevated risk for money laundering. In the future, to the extent that the underlying business process requires a KYC check, such KYC processes must also become a standard function in smart contract execution.

Blockchain may also enable innovative KYC solutions, e.g., self-governed identity, which will allow fully automated self-identification and whitelisting for frictionless b2b and b2c transactions. The integration of technologies such as zero-knowledge proof and cryptography will bring the privacy elements needed to protect personal and corporate information recorded on DLTs.

Several companies are currently working on the digitisation and blockchain solutions for all kind of documents used in logistics transportation. These will be the basis for not only sanctions and embargo screening of consignee, end-user and end use, but will also allow export licence checks/management as a smart contract function. Trade and export control compliance could be ensured by smart contract design and compliance managers should play an active role.

Summary and recommendation
The technology surrounding blockchain and decentralised smart contracts is still not yet at a stage where traditional companies can easily realise blockchain-enabled business processes or full blockchain-based business models. However, the technology has shown very promising use cases and is here to stay. We will see more and more business-ready solutions being developed, and it’s only a matter of time before we see large-scale adoption of certain elements of blockchain technology and smart contracts, chief among those being the ability to run software code on a decentralised system and ensuring the integrity of shared data.

If a company considers improving its business processes based on blockchain technology, its compliance managers should be involved from the onset to ensure the integration of trade controls into smart contract codes. This is a unique opportunity for enterprises to integrate compliance by design right from the initial design phase, ultimately reducing legal and financial risks, as well as the cost of compliance management.

Prof. Dr. Andreas Furrer is a legal partner at MME in Switzerland, where Peter Henschel is managing director of compliance and Chris Gschwend is a senior compliance advisor.

andreas.furrer@mme.ch
peter.henschel@mme.ch
christine.gschwend@mme.ch