

WorldECR

EO authorises sanctions against hackers	5
Caught in the 129 brokering trap	6
Sanctions biting business in Russia	8
Enforcement of export controls in the UK	12
New U.S. sanctions against Venezuela	15
South Korea's system of export controls	19
U.S. releases military drone export guidance	24
Navigating Israel's sanctions regime	28
IP network communications surveillance systems: deciphering Wassenaar controls	32
Listing dilemmas: a case study	38



German bank to double U.S. compliance staff in wake of \$1bn+ settlement

Germany's Commerzbank and its U.S. branch have agreed to forfeit \$563 million, pay a \$79 million fine, and enter into a deferred prosecution agreement with the U.S. Justice Department ('DoJ') for violations of U.S. regulations, the International Emergency Economic Powers Act ('IEEPA') and the Bank Secrecy Act ('BSA'), whilst also entering into settlement agreements with OFAC, The New York State Department of Financial Services and the Board of Governors of the Federal Reserve System, the DoJ has said.

Commerzbank has said that it is to double the number of U.S. compliance personnel it employs in an effort to improve its procedures.

According to the DoJ, in entering the deferred prosecution agreement, 'Commerzbank admitted and accepted responsibility for its criminal conduct in violation of IEEPA, and Commerz New York admitted its criminal conduct in violation of the BSA. Commerzbank further agreed to pay \$263 million in forfeiture and a fine of \$79 million for the IEEPA violations, and to pay \$300 million in forfeiture in connection with the BSA violations.'

\$1.45 billion in penalties

As has been the case in recent years, the bank was in the sights of more than one U.S. regulator. The DoJ noted: 'The New York County District Attorney's Office is also announcing today that Commerzbank has entered into a deferred prosecution agreement, and in the corresponding factual



Settlements relate to alleged transactions involving the bank and sanctioned Iranian and Sudanese parties.

statement, Commerzbank admitted that it violated New York State law by falsifying the records of New York financial institutions. In addition, the Board of Governors of the Federal Reserve System is announcing that Commerzbank has agreed to a cease and desist order, to take certain remedial steps to ensure its compliance with U.S. law in its ongoing operations and to pay a civil monetary penalty of \$200 million. The New York State Department of Financial Services (DFS) is announcing Commerzbank has agreed to, among other things, pay a monetary penalty to DFS of \$610 million. The OFAC has also levied a fine of \$258.6 million, which will be satisfied by payments made to the Justice Department. In total, Commerzbank will pay \$1.45 billion in penalties.'

Announcing the news to its shareholders, the bank said that since 2013 it had made changes in senior compliance personnel 'and plans to more than double US-based compliance staff by 2016.' It added: 'Efforts are underway to continue the introduction of more comprehensive global

compliance policies around the world.'

'Commerzbank concealed hundreds of millions of dollars in transactions prohibited by U.S. sanctions laws on behalf of Iranian and Sudanese businesses,' said Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division. 'Commerzbank committed these crimes even though bank managers inside the bank raised red flags about its sanctions-violating practices. Financial institutions must heed this message: banks that operate in the United States must comply with our laws, and banks that ignore the warnings of those charged with compliance will pay a very steep price.'

Increased compliance commitment

The bank's CEO, Martin Blessing said: 'We have made, and will continue to make, changes to our systems, training and personnel to address the deficiencies identified by U.S. and New York authorities. The U.S. dollar business remains a central component of our product suite to companies and financial institutions worldwide. As an

international bank, we have a keen interest in maintaining the highest industry standards everywhere we do business.'

Reid Whitten, an associate at law firm Sheppard Mullin, commented that the violation was 'consistent with a "broader problem" [the term employed by NY Financial Services Superintendent Benjamin Lawsky] with foreign-based financial institutions that have a U.S. presence.'

Whitten said, 'Transactions brought in by a European part of the company set off red flags with the U.S. entity's sanctions or AML software. The European branch then, instead of undertaking due diligence or rejecting the transactions that would create a violation in the U.S., acted to hide the illegality of the transaction with actions like wire-stripping. This reduces the number of red flags for the U.S. branch, which then does not examine why the red flags incidents are dropping.'

'The European entities think that the U.S. entities are being too cautious, that they are just crying wolf, so they make the problem worse by hiding things from the U.S. compliance function,' added Whitten, who drew attention to a comment made by a Commerzbank employee and quoted by the Department of Justice summary of the case: 'If for whatever reason CB [Commerzbank] New York inquires why our turnover has increase[d] so dramatically, under no circumstances may anyone mention that there is a connection to the clearing of Iranian banks!!!!!!!!!!!!!!.'

Cuba delistings not related to programme changes, but ‘in line’ with policy

OFAC has deleted 45 individuals and companies (Cuban and Panamanian) designated under its Cuban sanctions programme from its SDN list. OFAC said: ‘While these removals are not related to the recent changes to our Cuba sanctions program and rather reflect OFAC’s consistent effort to review and update its SDN list, these delistings are in line with the President’s Cuba policy.’

Observers have noted that some of those whose names have been removed are long deceased: Amado Padron Trujillo, for example, was executed by firing squad in 1989 by the Castro regime for his role in sending drugs to the United States. Reuters notes that the vessels now lifted from the SDN list are ‘sunk’ or otherwise unusable.

Earlier this year, the U.S. government published amendments to the Cuba embargo regulations so as to ‘facilitate travel to Cuba for authorized purposes, facilitate the provision by travel agents and airlines of

authorized travel services and the forwarding by certain entities of authorized remittances, raise the limit on certain categories of remittances to Cuba, allow U.S. financial institutions to open correspondent accounts at Cuban financial institutions to facilitate the processing of other activities related to, among other areas, telecommunications, financial services, trade, and shipping.’

Moving forward, slowly Miami-based lawyer, Ambar Diaz, who specialises in U.S.-Cuba relations said that the decision ‘is obviously related to the new relationship between the two countries,’ adding: ‘In a way, the relaxation programmes have been in place for years – such as eliminating all the requirements for travel agencies to operate in Cuba – but they are all part of the same policy that shapes a new climate between the Havana and Washington. I believe that the U.S. authorities are simply being cautious as to what to say

regarding the reasons behind the changes. My guess is that since they are going faster than their Cuban counterparts, they don’t want to give the perception that they are eliminating the measures too abruptly.’

Diaz added that she sees more people interested in doing business with Cuba,

While the Cuban government has already begun to open up to private entrepreneurship, an increased availability of capital in the country will be slow-growing.

but that ‘unfortunately, the areas of business are the same as before: exporting medicine, food, agricultural items [while] the U.S. still cannot give credit to Cuba, which is what Cuba really needs. I do hope that this will change in the not so distant future.’

Cuba, she said, ‘has been against the embargo all

along, so they are embracing all changes and opportunities coming their way.’

Lawrence Diamond, a partner at Duane Morris in New York, observed that while the Cuban government has already begun to open up to private entrepreneurship, an increased availability of capital in the country will be slow-growing.

‘The Cuban government is not going to want to relinquish the power it has held over the past decades. Raoul Castro and his supporters are still claiming that Cuba is going to be a prosperous, sustainable – but ultimately socialist – society,’ he said.

Despite increased engagement between U.S. and Cuban authorities, which includes a number of official trips at the highest level, Diamond believes that a normalisation of relations between the two countries will be slow to emerge.

‘What happens over the next three to four months will be very telling as to how things progress,’ he said.

UK exports to countries of concern

A grouping of House of Lords committees in the UK, jointly comprising the Committees on Arms Export Controls (‘CAEC’), charged with scrutinising arms export policy, has asked the UK government to respond to the question as to whether ‘it will adopt a policy of explaining to Parliament and the wider public more fully why certain countries, such as

Saudi Arabia, are listed by the Business Department as a Priority Market for arms exports whilst simultaneously being listed by the Foreign and Commonwealth Office as being a country of major human rights concern’.

Inter alia, in its report CAEC has asked the

government to explain arms export licences to countries listed within the Foreign Office’s 28 Countries of Concern. In particular, it asks that the government state ‘whether it is satisfied that each of the 3,298 extant arms export licences to the Foreign and Commonwealth Office’s 28

Countries of Human Rights concern, valued at £5.2 billion, and each of the 833 extant arms export licences to the Committees’ Additional 7 Countries of concern, valued at £356.1 million, are currently compliant with all of the Government’s Arms Export Licensing Criteria.’

<http://www.publications.parliament.uk/pa/cm201415/cmselect/cmquad/608/60805.htm#a80>

Schlumberger hit with \$232 million fine for IEEPA violations

Oilfield services company Schlumberger Oilfield Holdings ('SOHL') will plead guilty to, and pay a \$232,708,356 penalty for, 'conspiring to violate the International Emergency Economic Powers Act (IEEPA) by willfully facilitating illegal transactions and engaging in trade with Iran and Sudan.' So says the U.S. Department of Justice ('DoJ').

The DoJ says that the plea agreement, contingent upon court approval, also requires the company to submit to a three-year period of corporate probation, and to 'agree to continue to cooperate with the government and not commit any additional felony violations of U.S. federal law'. SOHL's parent company, Schlumberger Ltd., has agreed to terms that include:

- maintaining its cessation of all operations in Iran and Sudan;
- reporting on the parent company's compliance with sanctions;
- responding to requests to disclose information and materials related to the parent company's compliance with U.S. sanctions laws when requested by U.S. authorities; and
- hiring an independent consultant to review the parent company's internal sanctions policies and procedures and the parent company's internal audits focused on sanctions compliance.

The plea follows an investigation led by the Justice Department's National Security Division, the U.S. Attorney's Office



The company 'conducted business with Iran and Sudan from the United States and took steps to disguise those business dealings.'

for the District of Columbia and the U.S. Department of Commerce's Bureau of Industry and Security ('BIS') Dallas field office.

Assistant Attorney General John Carlin said, 'Over a period of years, Schlumberger Oilfield Holdings Ltd. conducted business with Iran and Sudan from the United States and took steps to disguise those business dealings, thereby willfully

The plea agreement, contingent upon court approval, also requires the company to submit to a three-year period of corporate probation.

violating the U.S. economic sanctions against those regimes.'

Commenting on the matter, Carlin added: 'The International Emergency Economic Powers Act is an essential tool that the United States uses to address

foreign threats to national security through the regulation of commerce. Knowingly circumventing sanctions undermines their efficacy and has the potential to harm both U.S. national security and foreign policy objectives. The guilty plea and significant financial penalty in this case underscore that skirting sanctions for financial gain is a risk corporations ought not take.'

Authorities getting bolder

Writing in a client alert, Scott Flicker, litigation partner at the Washington, DC office of law firm Paul Hastings, commented that the Schlumberger case proved that 'authorities are not only becoming more comfortable and more emboldened to bring large criminal cases, they are also armed with more information about how global business is conducted than at any previous time in the history of the sanctions and export controls enforcement programs.'

He said, 'the details of the

Schlumberger plea agreement reveal several important points. Along with the usual stipulations waiving indictment, accepting the factual narrative of the government and agreeing to pay fines and forfeiture penalties, both SOHL (the defendant) and Schlumberger Ltd. (its parent) agreed to sweeping provisions allowing the government extraordinary access to their operations. For example, SOHL and its parent agreed to disclose and, "as requested by the Government," provide all non-privileged information and materials, and to make available for government interviews and testimony all personnel, in connection with "any and all matters concerning any act within the scope of or related to the conduct" that was the subject of the investigation "or relating to other potential violations of sanctions pursuant to" the International Emergency Powers Act occurring during a three-year probationary period.'

Flicker pointed out that while such stipulations aren't unusual, 'in the context of the current raft of trade controls prosecutions, they underscore that the government's body of knowledge is growing about how transnational companies conduct global business, including with sanctioned jurisdictions. There can be little doubt that the investigations of today are generating substantial leads for the enforcement actions of tomorrow.'

Further information is at

<http://www.justice.gov/opa/pr/schlumberger-oilfield-holdings-ltd-agrees-plead-guilty-and-pay-over-2327-million-violating-us>

Executive order authorises sanctions against cyber-threats to U.S.

U.S. President Barack Obama has signed an executive order ('EO') that authorises the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States, 'and that have the purpose of:

- a) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- b) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- c) causing a significant disruption to the availability of a computer or network of computers; or
- d) causing a significant misappropriation of funds or economic resources, trade secrets,



President Obama blogged: 'Our primary focus will be on cyber threats from overseas.'

personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

The EO also authorises the imposition of sanctions against those 'responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by

a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability

of the United States.'

In his blog, President Obama wrote: 'Our primary focus will be on cyber threats from overseas. In many cases, diplomatic and law enforcement tools will still be our most effective response. But targeted sanctions, used judiciously, will give us a new and powerful way to go after the worst of the worst. Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit. From now on, we have the power to freeze their assets, make it harder for them to do business with U.S. companies, and limit their ability to profit from their misdeeds.'

<https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>

<https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know>

<https://medium.com/@PresidentObama/a-new-tool-against-cyber-threats-1a30c188bc4>

PayPal settles charges with \$7.7m penalty

Online payment services provider Paypal has agreed to pay just over \$7.6 million to settle a potential civil liability for apparent violation of several sanctions programmes administered by OFAC, including: the Weapons of Mass Destruction Proliferators Sanctions Regulations ('WMDPSR'); the Iranian Transactions and Sanctions Regulations ('ITSR'); the

Cuban Assets Control Regulations ('CACR'); the Global Terrorism Sanctions Regulations ('GTSR'); and the Sudanese Sanctions Regulations (SSR).

In an enforcement notice, OFAC said: 'For several years up to and including 2013, PayPal failed to employ adequate screening

technology and procedures to identify the potential involvement of U.S. sanctions targets in transactions that PayPal processed. As a result of this failure, PayPal did not screen in-process transactions in order to reject or block prohibited transactions pursuant to applicable U.S.

economic sanctions program requirements.' OFAC said that PayPal 'demonstrated reckless disregard for U.S. economic sanctions requirements' and that PayPal agents 'engaged in a pattern of conduct by repeatedly ignoring certain warning signs about potential matches to the SDN List'.

http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal.pdf

Caught in the 129 brokering trap

Export controls lawyer and sometime *WorldECR* contributor, Matthew Goldstein has filed a complaint with the U.S. District Court of Columbia against the U.S. State Department's Directorate of Defence Trade Controls ('DDTC'). The complaint is the culmination of Goldstein's efforts to clarify whether lawyers' services are covered by changes to brokering rules contained in Part 129 of the ITAR – as contained in an Interim Final Rule concerning the licensing of brokers, brokering activities, and related provisions published by the DDTC in 2013.

Goldstein, who says he has endeavoured – but failed – to receive an advisory opinion on the matter, describes his efforts to date to obtain clarity as 'Kafka-esque'. He warns that in the absence of a change in the current Proposed Rule lawyers will not be able to advise on ITAR-related defence exports whilst fulfilling their fiduciary duties to clients.

Background

The brokering story starts just less than two decades ago, when the U.S. Congress amended section 38 of the Arms Export Control Act ('AECA') in 1996 to close a loophole that emerged with details of brokering activities undertaken by the allegedly rogue CIA agent Edwin Wilson who arranged sales of defence articles and defence services to former Libyan President Muammar Gaddafi.

Previously, the AECA covered exports and re-exports of U.S. defence articles and defence services, but not activities by U.S. persons who brokered



Washington, DC attorney Matthew Goldstein has described his efforts to get clarity on the matter as 'Kafka-esque'.

foreign defence articles, unless those foreign defence articles came into the United States.

In October 2013, the International Law section of the American Bar Association ('ABA') sent the DDTC its comments on the Final Rule, praising the agency in large part for its efforts resulting in the exclusion of certain activities from the definition of brokering activities and for narrowing the scope of

'It is ... difficult to imagine the need for imposing Part 129 requirements on legal assistance when the underlying transactions already require application to DDTC for approval.'

'brokering activities' to actions taken 'on behalf of another' rather than actions that, while not explicitly taken on behalf of another, would benefit that person.

Nonetheless, it retained some significant concerns, amongst them, the application of Part 129, as iterated in the Interim Final Rule, to legal assistance provided by attorneys. In part, it was alarmed by a statement made by a DDTC official that certain forms of legal services by attorneys, such as advice on how to structure transactions involving sales of defence articles and the preparation of contracts and other documents for such transactions, would be caught by 129.

In its comments, the ABA International Law Section noted: "To date, Part 129 has not been applied to the provision of legal assistance by attorneys, but does currently capture conduct by attorneys outside the scope of legal services, such as the receipt of finder's fees for introductions. Consistent with this, revised Section 129.2(b)(2)(iv) of the Interim Final Rule provides an exclusion from Part 129 brokering requirements for "activities by an attorney that do not extend beyond

the provision of legal advice to clients."

Further, it points out that 'the Supplementary Information section of the Interim Final Rule provides that the "legal advice" referenced in the rule includes export compliance advice by an attorney to a client but that "By specifically calling out the type of advice it considers as falling under the exclusion, the Interim Final Rule implies that other forms of advice might not fall within the exclusion."

And: 'On its face, the exclusion does not seem to extend to communications by attorneys with parties on acquisitions, execution of agreements, and similar activities not exclusively involving "advice by an attorney to a client." Not including these forms of assistance in the scope of the exclusion for legal services is inconsistent with the realities of practicing export compliance law.'

Unrestricted access to counsel to advise on the legality of transactions, communicate legal requirements to third parties, and prepare legal documents, argued the ABA, 'is very much consistent with U.S. national security and foreign policy objectives because it helps ensure U.S. laws are being followed. In contrast, DDTC has not identified any foreign policy or national security interests threatened by such legal assistance... It is ... difficult to imagine the need for imposing Part 129 requirements on legal assistance when the underlying transactions already require application to DDTC for approval.'

Further, the ABA had considerable reservations concerning the way that

revised section 129.2(a)(3) of the Interim Final Rule applies. Part 129 requirements to foreign persons located outside the U.S. brokering foreign defence articles ‘solely based on their being owned or controlled by U.S. persons,’ which ‘creates substantial extraterritorial application of law problems in cases of legal assistance not excluded from Part 129.’

‘For instance,’ it argues, ‘an Australian law office that is “owned or controlled by” a U.S. firm and that participates in the negotiation of a domestic sale of defense articles from an Australian manufacturer to the Australian Ministry of Defense would be required to register as a broker with DDTC under the Interim Final Rule, although there is no export or import, much less any good or service coming from or going through the United States.’

The impacts of the provision as enshrined by the Interim Rule include, said the ABA, the following:

1. Companies are less likely to seek legal advice on matters when the information provided to attorneys is not confidential.
2. Companies are less likely to seek legal advice on time sensitive matters if they have to wait for DDTC prior authorisation before assistance can be provided.
3. Attorneys are unlikely to undertake representations that subject client records to warrantless searches by law enforcement under sections 122.5 and 129.11.

Advisory request

Matthew Goldstein’s further involvement in the 129 saga began when, in August 2013, he submitted a request for an advisory opinion from

the DDTC asking which of the following services offered by his firm ‘would be considered as brokering activities by the DDTC’:

- Advising how to structure transactions involving the sale of defense articles and defense services; to include advising how to structure sales, mergers, acquisitions and divestitures that involve the transfer of defense articles and defense services;
- Preparing contracts for the sale of defense articles and defense services, to include clauses, parts, and other provisions to contracts, as well as letters of intent, nondisclosure, and other documents incidental to contracts for sale, mergers, acquisitions, and divestitures;
- Advising on and preparing technical assistance agreements and other Part 124 agreements, to include advising on how to structure the involvement of subcontractors, sub-licensees, and other parties to Part 124 agreements;
- Advising on the availability of financing for export sales of defense articles and defense services, and preparation of legal documents required by financial institutions for financing of export sales of defense articles and defense services; preparing proposals and clauses, parts, and other provisions to proposals; and
- Corresponding and meeting with U.S. government personnel regarding licensing policy and specific requests to export defense articles and defense services.

Goldstein told *WorldECR*

that nearly a year after submitting his request, he still had not received a written answer from the agency. However, after he made repeated emails and telephone calls to DDTC for information on status of the request, he did receive a telephone call on 3 July 2014 from an agency official, with whom he discussed his concerns. According to Goldstein, this call lasted over 30 minutes, during which time the official assured him that none of the activities described in the advisory opinion request were subject to Part 129. Subsequently – and in the

**Goldstein told
WorldECR that
nearly a year after
submitting his
request [for an
advisory opinion], he
still had not received
a written answer
from the agency.**

light of the official’s assurances – Goldstein followed up with a letter to the official stating that he took his advisement (made by telephone) to mean that the activities above – provided that no fee arrangements were made on a commission or contingency basis – did not constitute brokering activities and requested the official advise him immediately if that understanding was incorrect.

In February this year, seven months after the July 3 telephone conversation, Goldstein received a letter from the same official advising him that his request for advisory opinion and the telephone conversation ‘lacked sufficient detail for the Department to make an official determination as to whether the activities constituted brokering

activities’ – and referred him to the very general advice given by the Department’s FAQs – the lack of specificity of which mirrored the same ambiguities in the Interim Final Rule that Goldstein had sought to clarify. To Goldstein’s incredulity, he says, the official also invited him to submit an advisory opinion request.

The complaint

On 9 March, Goldstein lodged his amended complaint, seeking injunctive relief prohibiting DDTC from applying its brokering rules to the provision of specified types of legal advice.

He says that if the government prevails in the lawsuit, he and others in his position will not be able to advise on many transactions involving the ITAR because to do so would necessitate breaching client confidentiality and the attorney-client privilege.

In addition, Goldstein advises that ‘the failure of DDTC to clearly state what legal services are subject to Part 129 violates the principle that the law must be transparent, certain, and provide adequate notice of what is prohibited.’

He further told *WorldECR*, ‘It’s an issue that many other people are concerned about – including law firms – but many are either afraid of what answer they’ll receive or they’re afraid of taking on the DDTC because of the agency’s reputation for vindictiveness.’

In his blog, well-known trade lawyer Cliff Burns said Goldstein should prevail: ‘DDTC’s bizarre volte-face on the applicability of Part 129 to legal services is unlikely to be favorably viewed by the court and means, I think, that the initial advantage in this lawsuit is with the plaintiff.’

Inside Moscow: sanctions begin to bite

Since the end of the Cold War, the Russian capital Moscow has, albeit in fits and starts, acquired a sophisticated commercial legal industry. Much early investment was premised on the (assumedly) inexorable convergence between the economies of Russia and the rest of the world, both in shape and the extent of their mutual dependence. Now, outlooks of East and West look increasingly at odds and those Moscow law firms find themselves administering triage to businesses wounded in the ongoing conflict between the two.

It is true that sanctions are only part of the parcel affecting the Russian economy – the fall in the price of oil and gas upon which it is pinned is also at play, and at least one lawyer says they observed a fall-off in investor interest at least a year before the imposition of sanctions. And yet the measures are clearly taking their toll.

Mikhail Kazantsev, a partner at law firm Egorov



Lawyers in Moscow report that sanctions against Russia are causing severe damage to international trade and investment.

Puginsky Afanasiev & Partners in Moscow, describes the financing and refinancing restrictions imposed on western lenders as starting to make major inroads into the ability of local companies to remain viable.

It's a widespread observation. Stefan Weber, of German law firm Noerr, and a veteran of the Moscow legal market, reports a significant escalation in businesses facing payment problems: 'There's increasing talk about extension of payment deadlines and revisions of existing supply contracts in the hope of enforcing payment claims.'

According to Weber, the majority of foreign investments are frozen, and that those companies moving forward 'are doing so cautiously, and building exit opportunities into their contracts'.

The observation is echoed by the observation of Suren Avakov, a lawyer at Avakov Tarasov & Partners, that both present and potential investors are going slow or not at all, and by Evgeny Zhilin, of the law firm Yust, who points out that the rise in the number

of disputes can be attributed to the fact that 'refinancing options are severely limited,' with state-controlled banks the only lenders liquid enough to finance business.

Meanwhile, Zhilin says, much of the debt held by private banks is – given a weakening economy and a hike in interest rates to around 20% – on the cusp of turning bad.

Against this backdrop, says Anton Nakou of Castrén & Snellman, a Finnish law firm with offices in Moscow and St. Petersburg, the number of clients seeking advice as to whether the sanctions qualify as circumstances that entitle them to claim *force majeure*, thus releasing them from their contractual obligations, has also risen.

Nakou says he's also advising companies that are looking to reduce their Russian operations or even pull out of the country entirely. Business development, it seems, is almost non-existent at the moment, with shareholders struggling simply to keep their businesses running, rather than develop them. Another outcome, Nakou says, has been a growing trend for non-designated share-

holders to urge designated parties to divest their holdings – and thus 'decontaminate' companies that would otherwise constitute risky business partners for EU and Western businesses.

Other alternatives?

Left with no borrowing options from the West, companies and banks touched by sectoral sanctions are looking east for alternatives, with Chinese, Singaporean, Hong Kong, Japanese and Middle Eastern lenders apparently pleased to take advantage of opportunities and, in the long term, some commentators believe these will win out over western lenders and investors.

'Russians have a real strength as a population,' says Evgeny Zhilin. 'They are very adaptable. Hard times provide good grounds for quick minds, and I believe that very soon the overall investment climate will start to grow.'

Stay vigilant

For now, talk of green shoots is premature. Vadim Nikitin of Stroz Friedberg, a risk and business intelligence information firm based in London, encourages companies to remain vigilant and keep up good compliance and due diligence processes, regardless of what happens at a geopolitical level. 'Companies need to make sure that they know exactly who they are dealing with in Russia,' says Nikitin. 'This is crucial as they could be potentially circumventing sanctions, hiding beneficial ownership through offshore accounts, proxy directives and registering companies in larger jurisdictions like Latvia and Cyprus.'

Russian returns

Russia, of course, has hit back at EU Member States by banning the import of some food products – resulting thus far in the loss of €21 billion worth of exports from the EU. Of Russia's counter-measures, Iain MacVay, a partner in King & Spalding's international trade practice observes, 'The EU Commission is currently struggling to decide on whether to challenge them. There is a strong argument that Russia's sanctions are illegal under WTO terms – but Russia contends that they are covered by security exceptions, making it difficult for the EU to move forward.'

The WorldECR Awards 2015

WorldECR is delighted to announce the launch of a set of Awards for the export control and sanctions community. The WorldECR Awards will 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 these inaugural Awards. Nominations should be sent to Awards@WorldECR.com, to reach us by Friday 10 April 2015. Winners will be announced in our June 2015 issue.

Nominations, which can include self-nominations and need not be limited to one individual per organisation, 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 600 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 the 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 will 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 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.

9) EXPORT CONTROL PRACTITIONER OF THE YEAR

This award recognises truly exceptional individual contributions to the development and implementation of good practice in export controls. The winner will have shown vision and either (1) great management skills and the ability to place the export control 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 to the global community.

10) 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

Nominations will be short-listed by Tom Blass, Editor, and Mark Cusick, Publisher, of WorldECR. Winners will be selected by our panel of Judges: Arnoud Willems, Partner, Sidley Austin; Daniel Martin, Partner, Holman Fenwick Willan; Fredrik Hallgren, Director of Group Trade Compliance, Ericsson; Jeff Snyder, Partner, Crowell & Moring; John Grayston, Partner, Grayston & Company; John Pisa-Relli, Managing Director of Trade Compliance, Accenture; Kay Georgi, Partner, Arent Fox; Kevin Cuddy, Export Controls Manager, GE Corporate; Laurence Carey, Group Trade Control Manager, Marshall Aerospace & Defence Group; Mario Mancuso, Partner, Fried Frank; Sandra Strong, Partner Strong & Herd; Scott Sullivan, Vice President – Ethics, Compliance & Legal, Flowserve Corporation.

Please note: judges will not be involved in the judging of awards for which they or their organisation have been shortlisted. All questions regarding these awards should be directed to awards@worlddecr.com



UNSC moves for South Sudan sanctions

On 3 March, the UN Security Council announced it had created 'a system to impose sanctions on those blocking peace in South Sudan.' However, according to reporting by the UN news service, some Council members warned that the move 'could derail Inter-governmental Authority on Development (IGAD) negotiations aimed at securing a deal by 5 March.'

Nonetheless, the Council condemned 'flagrant'

violations of the Cessation of Hostilities Agreements signed by South Sudan and the Sudan People's Liberation Movement ('SPLM'), expressing 'deep concern at the failure of both parties to honour their commitments, engage in the peace process towards political resolution of the crisis and end the violence.'

Amongst the measures that the UNSC says it could take are 'for example, [the imposition] for an initial

one-year period, of a travel ban on individuals, and an asset freeze on individuals and entities designated by a Sanctions Committee...for an initial 13 months.'

Actions that might trigger those measures, the UNSC said, include 'those aimed at expanding or extending the conflict, or obstructing peace talks; threatening

transitional agreements or the political process; planning, directing or committing acts that violated international humanitarian and human rights law, or human rights abuses; and targeting civilians or attacking hospitals, religious sites or locations where civilians sought refuge.'

<http://www.un.org/press/en/2015/sc11805.doc.htm>

Two years for breaching U.S. sanctions on DPRK

A Taiwanese businessman who pleaded guilty last October to conspiring with others to 'interfere with and obstruct U.S. regulations that seek to disrupt the proliferation of weapons of mass destruction,' has received a two-year sentence imposed by an Illinois judge, Judge Norgle, on 16 March.

Judge Norgle did however credit Hsien Tai Tsai 'for the substantial assistance he provided, and would continue to provide, to the government in its

investigation of weapons of mass destruction proliferators.'

Tsai was arrested in May 2013 in Estonia and extradited to the United States, where he remains in custody. Court documents say Tsai was associated with three companies based in Taiwan – Global Interface Company Inc., Trans Merits Co. Ltd., and Trans Multi

Mechanics Co. Ltd. – and that these 'purchased and then exported, and attempted to purchase and then export, from the United States and other countries machinery used to fabricate metals and other materials with a high degree of precision.'

Assistant Attorney General John Carlin said, 'Hsien Tai Tsai violated a

critical sanctions regime and undermined and interfered with U.S. efforts to disrupt North Korea's weapons of mass destruction and advanced weapons programs...This prosecution makes clear that we will use all of our tools to identify and arrest WMD proliferators and to disrupt their efforts to undermine our country's security.'

<http://www.justice.gov/opa/pr/taiwan-businessman-sentenced-24-months-conspiring-violate-us-laws-preventing-proliferation>

California man charged with illegal Russia exports

A Russian émigré and naturalised U.S. citizen ordinarily resident in San Francisco has been indicted for attempting to smuggle controlled U.S. electronic components, including dual-use programmable computer chips, to Russia out of San Francisco international airport, according to the Department of Justice, which says that Pavel Semenovich Flider, co-owner of Trident International Corporation,

'procured electronic components from U.S. companies and smuggled them to Russia using transshipment points in Estonia and Finland, in violation of U.S. export law.'

It said that Flider and Trident 'are alleged to have knowingly submitted false and misleading export

information on Shipper's Export Declarations, an official document submitted to the Department of Homeland Security in connection with export shipments from the U.S.'

Flider has been charged with 15 counts of smuggling of goods in violation of 18 U.S.C. § 554(a), one count

of conspiracy to commit international money laundering in violation of 18 U.S.C. § 1956(h) and ten counts of substantive money laundering in violation of 18 U.S.C. § 1956(a)(2)(A), according to DoJ.

Trident has been charged with the smuggling and money laundering charges.

<http://www.justice.gov/usao-ndca/pr/san-francisco-man-and-company-indicted-smuggling-sophisticated-electrical-components>

Japan extends North Korea sanctions

The Japanese government is extending its unilateral sanctions against North Korea – adopted in 2006 – by two years, according to reports from Japan's NHK news agency. The sanctions were set to expire on 13 April.

According to NHK, at a 31 March cabinet meeting ministers approved extending the trade embargo and

the banning of North Korean vessels from entering Japanese ports except for humanitarian purposes. It is understood this action has been taken because North Korea has failed to make headway with an investigation intended to reveal the fate of missing Japanese citizens in the DPRK, some of whom were abducted by the regime in

Pyongyang. At the onset of the investigation last July, Japan partially lifted the embargo.

On account of the lack of progress to date, Foreign Minister Fumio Kishida told reporters following the cabinet meeting, Japan 'will steadily implement the sanctions and use pressure and dialogue to resolve the abductions and other

pending issues,' and that the government 'will continue to consider the most effective way to use sanctions in realising the return of all abductees,' said NHK.

For more detail on Japan's current sanctions regimes, see 'Transition time in Tokyo', in issue 36 of *WorldECR* or the WorldECR Archive.

UK ECO to cheer up let-down electronics exporters

The UK's Export Control Organisation ('ECO', part of BIS, the Department of Business Innovation and Skills) has published a report compiled by trade association techUK on export controls process for UK-based electronic component and systems manufacturers. ECO says it intends to 'implement change to improve the export controls environment' by way of response.

In its report, techUK says it has identified a number of areas 'which can impact negatively on UK exporters along with the actions that

can be implemented to improve business opportunities'.

Amongst its findings, it says that 'Within the UK PCB [printed circuit board] industry, which is well regarded for export of high-end products to Europe, USA and Asia, companies reported lost and cancelled orders during 2014, due to export licence issues, amounting to 20% of their previous year's exports.'

techUK added: 'All but one company surveyed stated that the current enforcement regime in the UK has a negative impact

upon their export business compared to similar companies or branches of the same company located in the EU and/or USA.'

ECO has published an interim response in which it commits to 'support change in a number of areas, including:

- Bringing forward proposals to re-introduce a Control List Classification advice service;
- Examining ways to

introduce improved and more flexible open licensing solutions to meet exporter requirements; and

- Undertaking a review of end-user undertakings to determine options for ensuring UK exporters are not unnecessarily disadvantaged.

BIS welcomed the report as a part of its initiative to make regulations better for business.

<http://www.techuk.org/insights/news/item/3762-techuk-s-report-on-export-controls-published-by-bis>

The UK Institute of Export and International Trade

The Institute of Export and International Trade ('IOE') is the only professional body in the UK offering recognised, formal qualifications in international trade. IOE supports the interests of UK companies trading globally.

Established in 1935 and proud of its track record in providing members with a unique range of benefits, IOE seeks to enhance the UK's export performance by setting and raising professional standards in international trade management and export practice.

Dedicated to continuous development and best practice, IOE recognises and understands the challenging and often complex trading conditions members encounter across international markets.

In the knowledge that real competitive advantage lies in equipping those in international trade with knowledge, commerciality and key skills including negotiating power, IOE provides wide-ranging training programmes. For those

who want a more comprehensive knowledge of international trade, IOE provides a range of professional qualifications in international trade at various levels, up to Master's Degree. Accredited by Ofqual and designed to fit around a full-time career, IOE qualifications demonstrate commitment and expertise in international trade.

IOE's business membership package is aimed at smaller businesses and offers discounts on legal services, insurances, communication packages, foreign exchange processing and training. Other benefits include a members' advice line, set up to help exporters through any crisis, discounts on insurance, and a range of meetings and presentations.

UK businesses wanting to find out more about IOE, its training programmes and the wide range of members' benefits, should visit the website at www.export.org.uk or telephone +44 (0) 1733 404400.



PENALTY SPOT

In the first of a regular series of features in which *WorldECR* examines enforcement issues and trends, this month we look at **enforcement of export and trade controls in the UK.**

Of the EU's 28 Member States, the UK is regarded as one of those most proactive in terms of its engagement with export control issues and its willingness and capacity to enforce the law. And yet – as elsewhere in Europe – evidence of enforcement remains elusive and anecdotal – perhaps even frustratingly so. In part for this reason, an influential Parliamentary Committee has recently asked the UK government to provide a roadmap as to how it intends to address business non-compliance with export control regulations – and in no uncertain terms.

Enforcement framework

Certainly, the requisite infrastructure and process necessary for enforcement are in place. Suspected breaches of the export control regime are investigated by the Department for Business, Innovation and Skills ('BIS' – within which sits the Export Control Organisation or 'ECO'), Her Majesty's Revenue and Customs ('HMRC'), the UK Border Force – either singly, jointly or all three. The evidence gathered by these authorities is then passed on to an independent prosecuting body, the Crown Prosecution Service ('CPS'), which considers whether a decision to pursue criminal proceedings is in the public interest. In the case of successful prosecution, a confiscation order is made on the application of the prosecuting authority, compelling the

convicted defendant to pay a monetary penalty or 'recoverable amount'.

But white-collar crime lawyer and Corker Binning partner Andrew Smith says that despite a more aggressive stance pursued by regulators in recent years when it comes to violations of export and trade controls, criminal enforcement and prosecutions continue to be rare. He believes that

An influential Parliamentary Committee has recently asked the UK government to provide a roadmap as to how it intends to address business non-compliance with export control regulations.

this is mainly due to a 'lack of resources given to the criminal investigations department within HMRC' – a small department compared to the authority's other branches.

'If the regulators do uncover evidence that they've been [committing violations] deliberately over a number of years, then of course they will continue with criminal prosecutions,' says Smith. 'Most cases they investigate are on a first defendant basis, i.e. often,

it is the first time a company has been in trouble, and this is usually down to ignorance about the export controls that apply. In those circumstances, British authorities take the view that it is disproportionate to pursue prosecution – it is far better to let them off with a warning, take some money, and encourage them to reform.'

Case matters

The Export Control Organisation does not publish details on every single case of enforcement – perhaps restricting its reporting to the more newsworthy cases, and the open-source information that is available is often outdated (the last case listed on the BIS website where a compound penalty was imposed dates back to June 2012, when an unnamed company was fined '£1,000 for alleged offences in relation to the export of controlled goods without licences between July 2007 and December 2008').

On behalf of the authorities, Tim Morris of the Customs Enforcement Policy team in HMRC referred *WorldECR* to the annual report for 2013 (the last of its kind to be published on the BIS website), which highlights the enforcement outcomes for 2013-14 as being:

- 450 seizures of strategic goods in breach of licensing requirements or

Continues on page 17



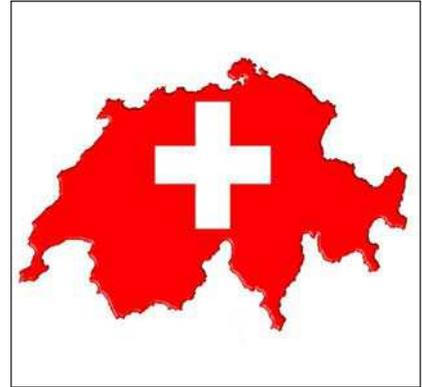
The WorldECR Archive at www.worldecr.com includes all past journal and website news PLUS every article that has ever appeared in WorldECR. If you would like to find out more about Archive Access, contact Mark Cusick, WorldECR's publisher at mark.cusick@worldecr.com

SWITZERLAND

Swiss publish Crimea circumvention measures

By Philippe Reich, Baker & McKenzie, Zurich

www.bakermckenzie.com



On 6 March, the Swiss government took measures to prevent the circumvention of the latest EU sanctions against Crimea and Sevastopol.

As part of these, Switzerland has added to its Ordinance on Anti-Circumvention of International Sanctions of 27 August 2014 the names of 28 individuals and entities who have been designated by the EU and they are therefore subject to the measures that Switzerland introduced following its non-recognition of Russia's annexation

of Crimea. As from 6pm on 6 March, financial intermediaries will no longer be able to enter into new business relationships with such persons and anyone in Switzerland with existing business relationships with them must notify SECO of such relationships.

The official press release also reveals that:

- all foreign investment into Crimea and Sevastopol is prohibited;
- service bans apply in the

investment, tourism and some other sectors;

- the existing ban on the export of key goods to Crimea and Sevastopol has been expanded; and
- the measures have been defined to more precisely align with the EU sanctions.

The Swiss Federal Council has warned that it 'continues to monitor the situation in Ukraine closely and reserves the right to introduce further measures'.

UK

House of Commons Committee keeps Iran listings under scrutiny

By Maya Lester, Brick Court Chambers

www.europeansanctions.com



The House of Commons European Scrutiny Committee has considered an EU Council decision to relist Gholam Golparvar and National Iranian Tanker Company on the EU's restrictive measures against Iranian nuclear proliferation. Their original listings were annulled by the General Court and the High Court refused to grant an injunction preventing their relisting. Both parties made submissions to the Committee objecting to their relisting, and the Committee has decided to retain the decision under scrutiny pending a review of how the matter has been handled by the government.

In a published statement, the Committee states that it asked the Minister for Europe, David Lidington MP, to explain why he could not

provide it with open-source information used to justify the relistings and to provide assurances that they were 'robust and could withstand legal challenge'. The Minister said the relistings are 'proportionate, adequately supported by open-source evidence, and consistent with Government policy towards Iran'. The Committee considers that this 'falls short of the confirmation he was invited to give', and 'strongly doubt that the

Council or Government will be able to enforce the confidentiality of open source material or sustain it if challenged'. It notes that 'In supporting the adoption of the relistings at Council, the Minister overrode scrutiny', and they 'do not accept that the override was unavoidable or justifiable'. The decision is 'characterised by mistakes and omissions' and the Committee has asked for the handling of the matter to be reviewed.

Links and notes

The EU Council decision is at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L._2015.039.01.0018.01.ENG

The Committee statement is at:

<http://www.parliament.uk/business/committees/committees-a-z/commons-select/european-scrutiny-committee/news/european-meeting-summary-18-march-2015/>

U.S.A.

New reporting requirements on the horizon for U.S. financial services providers doing business with non-U.S. persons

By Skadden, Arps, Slate, Meagher & Flom LLP; www.skadden.com



Following closely on the heels of the reinstated reporting requirements for inbound and outbound direct investment involving U.S. entities, the U.S. Department of Commerce's Bureau of Economic Analysis ('BEA') has announced plans to require U.S. financial service providers to respond to the Form BE-180 Benchmark Survey of Financial Services Transactions Between U.S. Financial Services Providers and Foreign Persons. As proposed, responses to Form BE-180 will be required by 1 October 2015, from all U.S. financial service providers

that, during their 2014 fiscal year, had financial transactions totalling \$3 million or more on a consolidated basis directly with non-U.S. persons (including individuals, corporations and other entities)¹. Failure to file a report can lead to civil and criminal penalties under the International Investment and Trade in Services Survey Act and related statutes.

Those likely to be affected by BEA's proposed new reporting requirements have an opportunity to make their voices heard. Specifically, BEA has requested written comments on the

proposed Form BE-180 reporting requirements by 30 March 2015. A final rule implementing such requirements is expected to be issued in advance of the proposed 1 October 2015 filing deadline.

As explained below, the scope of financial services subject to BEA's proposed reporting requirement is very expansive. Moreover, the proposed requirement casts a wide net to include any 'U.S. person' providing any type of financial service to non-U.S. persons.² For example, if implemented as currently drafted, the proposed reporting requirement would sweep in U.S. branches and subsidiaries of foreign entities as well as entities of various state, local and other governments that may offer financial services to non-U.S. persons.

The \$3 million reporting threshold proposed by BEA applies to the value of all transactions with foreign persons in the aggregate. Thus, even a U.S. financial service provider that had a large number of small-value transactions with many different foreign persons during its 2014 fiscal year would be required to report so long as the total value of all such transactions equalled or exceeded \$3 million. Moreover, in determining whether or not it meets the \$3 million threshold for reporting, a U.S. entity is required to add up the value of all financial service transactions engaged in by itself and each of its consolidated subsidiaries. As proposed by BEA, this means that a U.S. parent that otherwise does not offer any financial services would still be required to file a Form BE-180 if any of its U.S. subsidiaries bought financial services directly to, or sold financial services directly to, a foreign person and the total value of such transactions equalled or exceeded \$3 million on a consolidated basis.



EXPORT COMPLIANCE
TRAINING INSTITUTE
e-Seminars

Learn **WHEN, HOW & WHERE** it is convenient for **YOU!**

U.S. Export Controls & Embargoes
EAR, ITAR & OFAC Compliance Training

Train from your home or office computer... at **YOUR** convenience.

Now it is easier than ever to get the best in export compliance training for your company.

Easy to use e-Seminars include all of the content of our highly praised live seminars and combine:

- * Video instruction
- * Slides highlighting key concepts
- * Searchable, comprehensive e-Manual

Visit www.LearnExportCompliance.com/e-Seminars or call +1 540 433 3977 (USA) for details or registration.

Use Promo Code ECR-10 for 10% e-Seminar discount!

As proposed by BEA, the scope of reportable financial services transactions is very broad and includes:

- brokerage services, including those related to equity transactions;
 - underwriting and private placement services;
 - financial management services;
 - credit-related services, including credit card services;
 - financial advisory and custody services;
 - securities lending services; and
 - electronic funds transfer services.
- According to BEA, U.S. financial service providers coming within the scope of the proposed reporting requirement include providers of:
- depository credit intermediation (including commercial banking, savings institutions, credit unions and other depository credit intermediation);
 - non-depository credit intermediation (including credit card issuing, sales financing and other non-depository credit intermediation);
 - activities related to credit intermediation (including mortgage and non-mortgage loan brokers, financial transactions processing, reserve and clearinghouse activities, and other activities related to credit intermediation);
 - securities and commodity contracts intermediation and brokerage (including investment banking and securities dealing, securities brokerage, commodity contracts and dealing, and commodity contracts brokerage);
 - securities and commodity exchanges;
 - other financial investment activities (including miscellaneous intermediation, portfolio management, investment advice and all other financial investment activities);
 - insurance carriers, insurance agencies, insurance brokerages and other insurance-related activities;
 - insurance and employee benefit funds (including pension funds, health and welfare funds, and other insurance funds); and
 - other investment pools and funds (including open-end investment funds, trusts, estates, agency accounts, real estate investment trusts and other financial vehicles).

Links and notes

¹ BEA benchmark surveys are normally conducted every five years. The last BE-180 benchmark survey covered the 2009 fiscal year.

² As drafted, the requirement applies to 'each U.S. person that is a financial services provider or intermediary.' 'U.S. person' is defined by BEA as 'any person resident in the United States or subject to the jurisdiction of the United States,' and 'person' is defined as 'any individual, branch, partnership, associated group, association, estate, trust, corporation, or other organization ... and any government (including a foreign government, the United States Government, a State or local government, and any agency, corporation, financial institution, or other entity or instrumentality thereof, including a government-sponsored agency).'

Also covered are U.S.-based holding companies that own, or influence the management decisions of, firms principally engaged in the aforementioned activities.

U.S.A.

New sanctions programme creates risks for companies doing business with Venezuela

By Laura Fraedrich, Michael P. Gurdak, Fahad A. Habib, Chase D. Kaniecki and Lindsey M. Nelson, Jones Day
www.jonesday.com

On 9 March 2015, President Obama signed the Executive Order Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Venezuela, declaring the current situation in Venezuela a threat to national security and imposing sanctions on certain Venezuelan military and security officials. While

the sanctions are limited to certain individuals for now, companies, both foreign and domestic, doing business in the region should ensure that their compliance programmes capture the new sanctions to prevent possible violations.

U.S. companies with business involving Venezuela should ensure that



their activities do not relate to parties designated under the new sanctions. Non-U.S. companies engaged in business with or involving targeted parties face their own risks as sanctions may be imposed on persons or entities that provide material support to designated parties.

The executive order, promulgated in the wake of President Obama's signing of the Venezuela Defense of Human Rights and Civil Society Act of 2014 on 18 December 2014, was issued in response to 'the situation in Venezuela, including the Government of Venezuela's erosion of human rights

Links and notes

The executive order is at:

http://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_eo.pdf

The Defense of Human Rights and Civil Society Act is at:

<https://www.congress.gov/113/bills/s2142/BILLS-113s2142es.pdf>

guarantees, persecution of political opponents, curtailment of press freedoms, use of violence and human rights violations and abuses in response to anti-government protests, and arbitrary arrest and detention of anti-government protestors, as well as the exacerbating presence of significant public corruption' in Venezuela.

Pursuant to the new sanctions, the following persons may be designated on the list of Specially Designated Nationals and Blocked Persons ('SDN List') and blocked:

- Persons responsible for or complicit in, or responsible for ordering, controlling, or otherwise directing, or who have participated in: (i) actions or policies that undermine democratic processes or institutions; (ii) significant acts of violence or conduct that constitutes a serious abuse or violation of human rights (including against persons involved in anti-government protests in Venezuela in or since February 2014); (iii) actions that prohibit, limit, or penalise the exercise of freedom of expression or peaceful assembly; or

(iv) public corruption by senior officials within the Government of Venezuela.

- Current or former leaders of an entity that has, or whose members have, engaged in any activity described above, or of an entity designated under the sanctions.
- Current or former officials of the Government of Venezuela.

In conjunction with the executive order, the U.S. Department of the Treasury's Office of Foreign Assets Control ('OFAC') added seven Venezuelan military and security officials to the SDN List. Any entity owned 50% or more by one or more designated persons also is considered a designated party, regardless of whether the owned or controlled entity itself is designated on the SDN List.

U.S. companies engaging in activities in Venezuela generally are prohibited from any business activities that involve or otherwise relate to these designated individuals or any entities majority-owned by them. In addition, the designated persons are prohibited from entering the United States.

Finally, any parties, including non-

U.S. persons, also may be designated on the SDN List and blocked if they:

- materially assist, sponsor, or provide financial, material, or technological support for, or goods or services to or in support of, the above-described persons or activities; or
- are owned or controlled by, or act for or on behalf of any person designated under the sanctions.

Companies doing business with Venezuela should perform due diligence on existing or potential business partners, including customers, to confirm whether they are on the SDN List or owned or controlled by any designated parties.

As additional designations are possible, companies should also evaluate whether their business involves any of the categories of potential sanctioned parties, such as current or former officials of the government of Venezuela. This will allow companies to assess their current risk against an expansion of the sanctions or additions to the SDN List, and plan for contingencies if those occur.

U.S.A.

Government publishes notice on import of eligible Cuban goods and services

By Eunkyung Kim Shin, Christopher Lucas and Alexandre Lamy,
Baker & McKenzie
www.bakermckenzie.com

On 26 February 2015, U.S. Customs and Border Protection ('CBP') published a public notice on its website regarding the procedures for importations from Cuba recently authorised by the U.S. government. This notice establishes the processes (and requirements) by which both commercial goods and goods for personal use are to be imported into the United States. It is the latest component of the U.S. government's recent relaxation of the comprehensive U.S. embargo of Cuba.

Under section 515.582 of the Cuban Assets Control Regulations ('CACR'), persons subject to U.S. jurisdiction are authorised to engage in all transactions (including payments) necessary to import into the United States certain goods and services produced by independent Cuban entrepreneurs. The section 515.582 list, published by the State Department, provides the current list of eligible and excluded Cuban goods and services.

The CBP notice establishes the following requirements with regard to

the importation of such authorised goods from Cuba into the United States:

Importing commercial goods from Cuba

For importation of commercial goods (e.g., goods for retail sale in the United States), CBP requires a customs informal entry for goods valued at under \$2,500, and a formal entry for goods exceeding \$2,500. Under the 2015 Harmonised Tariff Schedule of the United States ('HTSUS'), Cuba is a



Column 2 country, and, as such, goods eligible for importation from Cuba are subject to Column 2 specific duty rates (as opposed to standard Column 1 duty rates). As a practical matter, Column 2 duty rates are significantly higher than standard Column 1 rates. Indeed, the duty rates on commercial goods eligible for importation from Cuba can reach 75% or more.

Importing goods for personal use from Cuba

- *Imports by authorised travellers of goods produced by independent Cuban entrepreneurs under CACR section 515.582:* Imports by individuals returning from Cuba as part travel authorised under the CACR are allowed an \$800 exemption from customs duties in accordance with the HTSUS, if the goods are for personal use. The first

\$1,000 above that \$800 (i.e., \$801 to \$1,800) will be assessed duty at a rate of 4%. The \$800 exemption and the application of the 4% duty rate for \$801 to \$1,800 will be multiplied by the number of qualified family members travelling in the same group.

- *Imports by authorised travellers of goods other than those authorised by CACR section 515.582:* For goods other than those authorised by CACR section 515.582, CACR section 515.560 imposes specific limitations on the total value that

may be imported into the United States. The value of merchandise purchased or otherwise acquired in Cuba that is imported as accompanied baggage may not exceed \$400 per person, of which no more than \$100 may consist of alcohol or tobacco (or a combination thereof). Products purchased for importation under CACR section 515.560 do not need to be sourced from independent Cuban entrepreneurs. Imports of alcohol and tobacco over the \$100 limitation will be detained or seized.

Links and notes

The CBP notice is at:

www.cbp.gov/travel/cbp-public-notice-process-imports-cuba

CACR s.515.582 is at:

http://www.ecfr.gov/cgi-bin/text-idx?SID=034b3150986b18c166edebc53094e097&node=se31.3.515_1582&rgn=div8

Continued from page 12

sanctions and embargoes (see table 5.III)

- 138 catch-all cases where goods subject to end-use control were prevented from leaving the UK
- Eight compound penalties paid to HMRC totalling £447,000

One successful criminal prosecution is also listed. In 2013, Christopher McDowell and Wellfind Ltd. were convicted of being knowingly concerned in the supply and transfer of K8 Fighter Aircraft and designated parts to Ghana with intent to evade the prohibition of such controlled goods. McDowell was found guilty on one count and sentenced to two years' imprisonment, suspended for two years on completion of 200 hours of community service.

More recently, in March 2014, Gary Summerskill was jailed for 30 months and his company, Delta Pacific Manufacturing Limited, ordered to pay £1,072,000 after an investigation by HMRC found he had attempted to conceal the illegal export of alloy valves to Iran (see *WorldECR* issue 36).

Perhaps the figures are not in themselves the whole story. James Robinson, a partner at UK law firm Eversheds points out that while 'the number of criminal prosecutions for export control breaches in the UK is relatively low – certainly in comparison to criminal enforcement in the U.S. – there has in recent years been a clear drive to demonstrate that the UK is actively monitoring compliance.' Robinson says that the UK appears to be increasingly recognising the value of voluntary disclosure in respect of potential breaches of export controls.

Another interesting exercise would be to contrast UK statistics with those of other EU Member States. That, however, is likely to remain an aspiration for some time: *WorldECR* understands that even the DG Commerce within the European Commission (responsible for export control policy) has yet to obtain enforcement records from most Member States – and that any further centralisation of enforcement-related activities has been explicitly excluded from the Commission's forthcoming review of the dual-use export control regime.

Types of penalties

Strict liability offences, such as the export or attempted export of controlled goods without a licence, can incur any one of a number of responses from the UK authorities, including:

- warning letters
- revocation of licences
- seizure of goods
- penalties of up to three times the value of the goods
- two years' imprisonment and,
- the issue of compound penalty fines

Where a company is found to deliberately act with intent to evade controls, a magistrates' court may order a penalty of £5,000 or three times the value of the goods (whichever is greater) and the imprisonment of responsible individuals for up to six months. Depending on the gravity of the offence, a crown court could also order defendants to face up to ten years' imprisonment or pay a 'compound penalty' of an unlimited amount – the latter offer companies the chance to settle a case that would otherwise justify being referred to the CPS for prosecution.

**SAVE THE DATES: THE WORLDECR EXPORT CONTROLS AND SANCTIONS FORUM 2015:
WASHINGTON, DC, 21-22 SEPTEMBER 2015; LONDON, 14-15 OCTOBER**

A time for strange bedfellows

The fitting subject of this editorial should of course be the outcome of the P5+1 talks with Iran. Unfortunately, the seven world powers involved in those negotiations declined a request to ensure that they adhered to the *WorldECR* publishing schedule.

And yet, in anticipation of any forthcoming announcement about general frameworks and agreements in principle, there's only so much that can be said on the subject. It would be trite to say that the outcome, whatever it may be, opens a new chapter in Middle East relations – for a new chapter is already far advanced. In Yemen, the Saudis are fighting Iran-backed Houthis in what is rapidly becoming described as a proxy war. In Iraq, Iran and the U.S. are both involved in assisting Baghdad in its fight against the Islamic State – against which the President of Syria, still in place three years after the then-Secretary of State declared 'Assad Must Go', is also at war. The U.S. and Russia negotiate on the same side against Iran as Security Council members, though in almost every other sphere relations between them have broken down. Meanwhile, the U.S. President cold-shoulders the re-elected Israeli Prime Minister for the assurances he gave his electorate that a two-state solution to the Palestinian question would not happen on his watch.

Currently, there are sanctions

against Iran, Syria, Yemen and Russia. In sum, this is a challenging global market in which to do business, and one overlaid with ironies.

Commerce, like nature, abhors a vacuum and flourishes even in the cracks between nation states and craters left by conflict. Three household names have hit the headlines for the

The ironies of politics – foreign and domestic – are as prevalent in the cyber-realm as they are on land and sea.

wrong reasons since *WorldECR* last went to press – a U.S. oilfield services firm, a German bank and a friendly and ubiquitous online payment facilitator.

I was struck by the recent comment of one lawyer in the wake of those enforcement cases that 'authorities are not only becoming more comfortable and more emboldened to bring large criminal cases, they are also armed with more information about how global business is conducted than at any previous time in the history of the sanctions and export controls enforcement programmes.'

Indeed, information has become an over-arching meta-commodity, the flow of which, like that of goods and

capital, can serve purposes good or ill. On 1 April, the U.S. President announced a new executive order authorising the imposition of sanctions against those responsible for 'malicious cyber-enabled activities constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States'.

On his blog, he wrote: 'It's one of the great paradoxes of our Information Age – the very technologies that empower us to do great good can also be used by adversaries to inflict great harm. The same technologies that help keep our military strong are used by hackers in China and Russia to target our defense contractors and systems that support our troops. Networks that control much of our critical infrastructure – including our financial systems and power grids – are probed for vulnerabilities by foreign governments and criminals.'

It's a bold statement, in the light of the Jewel lawsuit against the National Security Agency in an attempt to end dragnet surveillance of the communications and communications records of U.S. citizens, and a salutary reminder that the ironies of politics – foreign and domestic – are as prevalent in the cyber-realm as they are on land and sea.

Tom Blass, April 2015
TNB@worldocr.com



The WorldECR Archive at www.worldocr.com includes all past journal and website news PLUS every article that has ever appeared in WorldECR. If you would like to find out more about Archive Access, contact Mark Cusick, WorldECR's publisher at mark.cusick@worldocr.com

From policy to implementation: a review of South Korea's system of export controls



South Korea, a major producer and exporter of strategic items (and increasingly of arms) and a global trans-shipment point, first introduced export controls in the 1980s and recognises its considerable responsibilities to prevent proliferation. This article outlines the South Korean export control system, focusing on controls on WMD-related dual-use items. By Jaewon Lee.

The debate around export controls (whether to have them/how to formulate them) didn't come to South Korea until the late 1980s, when a mixture of international and domestic political dynamics generated a conflict in South Korean trade policy. On the one hand, a new policy emerged that emphasised political and economic relations with Communist countries, and South Korean companies increasingly demanded economic engagement with them, with the country achieving rapid economic growth driven by export-oriented industrialisation and seeking new markets in China, Eastern Europe and

the Soviet Union. On the other hand, this was seen as a challenge to U.S.-led efforts to exert more pressure to contain the declining economies of the Communist bloc. Moreover, by this time South Korean companies had reached a level of technological development that allowed them to produce goods (e.g. computers with 16-bit processors) that were controlled under COCOM (the Coordinating Committee for Multilateral Export Controls, established at the end of World War II to control the arms trade with Eastern Bloc and certain other countries). The U.S. thus approached South Korea on a bilateral basis to ask

it to comply with the COCOM guidelines in order to avoid a weakening of the effect of the existing multilateral containment policy. In 1987, South Korea and the U.S. signed an agreement 'to preclude the unauthorised transfer of such commodities and technical data to proscribed communist destinations'. In return for the establishment of a comprehensive export control system, South Korea was granted preferential licensing benefits by the U.S. government. The agreement served as a cornerstone for South Korea's establishment of export control regulations.



The South Korean government made slow progress in implementing the agreement. As a partial implementation, South Korea established a system to issue COCOM-style 'import certificate/delivery verification' ('IC/DV') documents through a presidential decree in 1987 under the Foreign Trade Act.

However, the South Korean government only started to operate the IC/DV system in 1990. In 1992 South Korea amended the Foreign Trade Act to include an additional sub-chapter authorising the Minister of Commerce to require permits for the export of strategic items. It was only in 1993 that the South Korean government announced a concrete plan to set up a legal and organisational framework for licensing authorities.

In the 1990s the U.S. came to consider export controls, which were no longer needed as part of a containment policy against Communist countries, as necessary for non-proliferation purposes. The U.S. was concerned that the new post-cold war order would weaken the impetus for South Korea to continue to implement export controls. However, the South Korean government had a keen interest in continuing export controls as part of its containment policy against North Korea. South Korea also had concerns about those former Communist countries that maintained relations with North Korea.

South Korea's national security interests were projected at the international level as a political commitment to the non-proliferation of strategic items, which led to South Korea becoming one of the original participants in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies in 1996. Participation was possible because of South Korea's normative approach to non-proliferation, its achievement of a certain level of production capabilities and enactment of the export control regulations required by the Wassenaar Arrangement.

South Korea also joined the other multilateral export control regimes: the Nuclear Suppliers Group ('NSG') in 1995, the Australia Group in 1996, and the Missile Technology Control Regime ('MTCR') in 2001. UN Security Council Resolution 1540 of 2004, which obliges all UN member states to establish measures to control the risk of

proliferation of WMD and their means of delivery, further stimulated the development of South Korea's export controls.

Legal structure and control lists

Four pieces of primary legislation form the basis of the current export control system in South Korea: the Foreign Trade Act, the Defense Acquisition Program Act, the Nuclear Safety Act, and the Act on the Control of the Manufacture, Export and Import of Specific Chemicals and Chemical Agents for the Prohibition of Chemical and Biological Weapons ('Prohibition of Chemical and Biological Weapons Act').¹

While each of these laws regulates a different type of item, the Foreign Trade Act serves as the main pillar of

Minister of Trade, Industry and Energy in consultation with the heads of the relevant administrative agencies, and published in the Public Notice.

The Public Notice also specifies the process for preparing and submitting a licensing application and contains two control lists of items.

Control lists of strategic items

Strategic items are listed in annexes 2 and 3 of the Public Notice. Export of the items in these two lists is subject to control under the four export control laws.³

In annex 4 of the Public Notice, the South Korean government provides a table that categorises such items under the four export control regimes and two international treaties – the Wassenaar Arrangement, the MTCR,



The Foreign Trade Act serves as the main pillar of South Korean export controls. It regulates who issues export permits and how the licensing procedure should be conducted.

South Korean export controls. It regulates who issues export permits and how the licensing procedure should be conducted. For example, article 11 of the Prohibition of Chemical and Biological Weapons Act requires exporters to obtain export licences in accordance with articles 19 and 26 of the Foreign Trade Act, while article 57(2) of the Defense Acquisition Program Act requires anyone who plans to export military items to obtain licences from either the Minister of Trade, Industry and Energy (in line with the Foreign Trade Act) or the commissioner of the Defense Acquisition Program Administration ('DAPA').

A single implementation system applies to all four laws, based on article 19 of the Foreign Trade Act and its Public Notice on Trade of Strategic Goods and Technologies.²

Article 19(2) of the Foreign Trade Act states that anyone who exports 'strategic items' must obtain an export licence from either the Minister of Trade, Industry and Energy or the head of the relevant administrative agency.

'Strategic items' which require export permits are designated by the

the NSG and the Australia Group and the 1972 Biological and Toxin Weapons Convention ('BTWC') and the 1993 Chemical Weapons Convention ('CWC').⁴

Annex 2 lists dual-use items, including items from the NSG trigger list with a solely nuclear use. Annex 3 lists conventional munitions (identical to the Wassenaar Arrangement munitions list).

These new control lists came into effect in 2008; previously, South Korea had maintained separate control lists for each export control regime. Items in the list are assigned a five-character alphanumeric code; the fourth (alphabetic) character and the fifth (numeric) character represent the category of the items; and the third (numeric) character indicates the relevant export control regime.⁵ South Korea's current coding method is thus similar to that used in the EU list of dual-use items (which is based on the Wassenaar Arrangement control list system) and to the Export Control Classification Number ('ECCN') used in the U.S. Commerce Control List.

The annexes are frequently updated to reflect changes in the lists of the four

multilateral regimes; amendments are issued through a notification from the Minister of Trade, Industry and Energy, in consultation with the head of the relevant administrative agencies.⁶

The South Korean lists include two

government largely regulates three types of controlled item: dual-use, munitions and exclusively nuclear items. Among these, munitions include two subcategories: general defence industry materials and major defence

Export of major defence industry materials found in annex 3 and any dual-use item in annex 2 where the importer intends to use it for a military purpose requires a licence from the commissioner of DAPA. Exports of dual-use items with a solely nuclear use in category 10 of annex 2 require licences from the head of the NSSC.¹²

Inter-agency coordination is provided by the Council for Control of Exportation and Importation of Strategic Items. Meetings of the council can be organised by the Minister of Trade, Industry and Energy and the heads of relevant administrative agencies – that is, the NSSC, the Ministry of Unification, the Ministry of Foreign Affairs and the Ministry of National Defense – for consultation among the organisations. The Council may request the intelligence, investigation or prosecution agencies – the National Intelligence Service, the Prosecution Service, the Korean National Police Agency, and the Defense Security Command – conduct an investigation or render assistance, if necessary, for any items on its agenda.

Identification services – that is, identification of which items are subject to export control – are provided by three agencies. KOSTI provides identification services for dual-use items. Identification services for the trigger list items (annex 2, category 10) are provided by the Korea Institute of



A transit and transshipment licence is required by anyone who is to transit or transship strategic items or items subject to a situational licence through South Korean harbours or airports.

items in addition to those listed by the regimes: severe acute respiratory syndrome ('SARS') coronavirus and bovine spongiform encephalopathy ('BSE') agent.

Defence industry materials

In addition to the conventional arms listed in annex 3, the South Korean government maintains another list for munitions, defined as 'defence industry materials' by the Defense Acquisition Program Act. Although the concept of the annex 3 munitions list and defence industry materials differ, since the two laws control the weapons according to different criteria, most defence industry materials are included in the list of 'strategic items' in annex 3.

Defence industry materials are defined to be 'weapons systems' that are designated by the commissioner of DAPA in consultation with the Minister of Trade, Industry and Energy as being 'necessary for the securing of stable source of procurement, strict quality assurance, etc.' – that is, items whose export needs to be controlled in order to secure a stable supply of high-quality arms for the South Korean government.⁷

Defence industry materials are divided into two groups: major items and general items. The Defense Acquisition Program Act designates 12 types of major defence industry item.⁸ All other defence industry materials are general defence industry materials.⁹

The commissioner of DAPA, in consultation with the Minister of Trade, Industry and Energy, is responsible for designation of contractors and classification of the products into categories.

In summary, the South Korean

industry materials. However, there could be conflicting definitions of the munitions list (annex 3) and 'defence industry materials', which would affect the identification and licensing process. Nonetheless, the three licensing authorities have a clear division of roles for issuing export permits for controlled items.

Licensing – agencies

There are three licensing authorities in South Korea's export control system, each issuing export licences for different categories of strategic item: the Minister of Trade, Industry and Energy, the commissioner of DAPA, and the head of the Nuclear Safety and Security Commission ('NSSC').¹⁰



Licence application documents can be submitted via Yestrade, the online national export controls system.

The export of dual-use items listed in categories 1-9 of annex 2 and general defence industry materials found in annex 3 (the munitions list) requires a licence from the Minister of Trade, Industry and Energy.

Licence application documents can be submitted via Yestrade, the online national export controls system developed by the South Korean Ministry of Trade, Industry and Energy ('MOTIE') and the Korea Strategic Trade Institute ('KOSTI').¹¹

Nuclear Nonproliferation and Control ('KINAC') on behalf of the NSSC. DAPA provides identification services within its department.

Since many conditions, with different perspectives, apply to export controls on 'unlisted' items (items not mentioned in control lists but which may be intended for use in a WMD programme), MOTIE provides an implementation process for catch-all clauses on Yestrade. When an item of concern is identified as not listed in the

Public Notice, exporters are asked to answer the following four questions to see if the item, end use and certain circumstances require a situational licence:

- 1) Is the importer or the end-user on the Denial List (searched via Yes-trade)?
- 2) Does the item and its destination appear in annex 2(2)?
- 3) Is a diversion of end use perceived?
- 4) Is the destination of the item a Group B country and does a situation listed in articles 39(1)1–12 of the Public Notice apply?

If the answer to any of these questions is 'yes', the exporter is required to apply for a situational licence. A transit and transshipment licence is required by anyone who is to transit or transship strategic items or items subject to a situational licence through South Korean harbours or airports. ('Transshipment' is defined as moving and loading goods from an arriving means of transport to another departing means of transport within the same customs jurisdiction.)

Until recently it was the case that for brokering licences, only strategic items (or listed items) were subject to control; in other words, the South Korean government did not apply a catch-all clause to brokering licences. This has now changed (see below). The Public Notice defines 'brokering' as any action conducted by any South Korean who is residing in South Korea (including legal persons established according to domestic laws) to transfer strategic items from one foreign country to another, when the transactions involve contracts for trade or other forms of transaction (including free transfer) with payment of commission or other compensation.

The Public Notice also regulates re-export of strategic items. Re-export is defined as the export of an imported strategic item in its original form or of manufactured or processed goods that incorporate imported strategic items (regardless of whether the new goods are strategic). If it is a new product that is not identified as a strategic item and the value of the imported strategic items is less than 25% of the new product or if the imported strategic item cannot be separated from the final product without losing its original functions, a re-export licence is not required.

Prosecutions, penalties and administrative measures

On initiation of a legal process, prosecutors have discretion to decide whether to bring a case to court, and the right to bring a case to court is solely decided by the Prosecutors' Office. As Anna Wetter (a researcher with the SIPRI Arms Control and Non-proliferation Programme until 2007) argues, 'in systems that grant prosecutorial discretion, it is crucial that prosecutors are convinced of the severity of a certain crime, since they may not otherwise choose to refer a case to the court'.¹³ Thus, the South Korean system, where detection by customs officers is not sufficient for prosecution, may not provide effective law enforcement.

In terms of criminal sanctions, the Foreign Trade Act provides two penalty provisions for export violations related to strategic items. First, anyone who exports items without a licence to facilitate international 'proliferation' of strategic items faces imprisonment for up to seven years or a fine not exceeding five times the value of the exported or brokered items. Second, anyone who exports items without a licence or who obtains a licence fraudulently faces imprisonment for up to five years or a fine not exceeding three times the value of the exported goods.

The first of these penalties emphasises specific offences that contribute to proliferation of strategic items, while the second is related to any unauthorised transaction. The two penalty provisions may not be different, because by definition illegal exports facilitate the international spread of strategic items. Moreover, 'proliferation' is normally used in reference to WMD, not strategic items, in the field of non-proliferation export controls. The legal expression used in this provision is thus unique. Penalties for crimes of negligence are not specifically mentioned. As an example of an enforcement case, in 2011 equipment for the production of shells was illegally exported to

Myanmar by 14 former and current staff members of a South Korean company that produces defence items.¹⁴ The offenders disguised shipments as agricultural machines. They were sentenced to prison terms of 12-18 months, suspended for 2-3 years. They were also fined between 5 and 50 million won (\$4,500-45,000).

In another example, between 2005 and 2008 a company exported around 200 dual-use machine tools without the necessary licences to China, India and nine other countries. The company was fined 50 million won (\$45,000) and received a one-month export restriction.

The Foreign Trade Act contains three administrative sanctions:

First, the Minister of Trade, Industry and Energy or the head of a relevant administrative agency can ban all exports or imports of strategic items for up to three years by a person who has exported any strategic items without an export licence or situational licence.

Second, the Minister of Trade, Industry and Energy or the head of a relevant administrative agency may issue an 'educational order' to take a training course of up to eight hours to (a) any person who has exported strategic items without an export licence or a situational licence or (b) any person who obtained an export licence or a situational licence by fraud or other wrongful means.

Third, a civil fine not exceeding 20 million won (\$18,000) can be imposed on any person who has failed to submit a report or data or has submitted a false report or data.

In 2011 the Minister of Trade, Industry and Energy ordered 21 administrative measures for violations of the Foreign Trade Act. These included warnings and educational orders for 15 companies, export restrictions of up to two months, and fines for three companies, and three cases where export and import restrictions were imposed for up to three months.

Recent developments

South Korea has facilitated the implementation of export controls, with agencies such as MOTIE assisting

companies in order to enhance the country's competitiveness on the global market. For example, MOTIE has helped prepare exporting companies

Links and notes

- ¹ Foreign Trade Act, Law no. 11 873 as amended up to 7 June 2013, <<http://www.law.go.kr/lsInfoP.do?lsiSeq=141071&efYd=20130701>> (in Korean); Defense Acquisition Program Act, Law no. 11 713 as amended up to 23 Mar. 2013, <<http://www.law.go.kr/lsInfoP.do?lsiSeq=137319&efYd=20130323>> (in Korean); Nuclear Safety Act, Law no. 11 715 as amended up to 23 Mar. 2013, <<http://www.law.go.kr/lsInfoP.do?lsiSeq=137336&efYd=20130323>> (in Korean); and Act on the Control of the Manufacture, Export and Import of Specific Chemicals and Chemical Agents for the Prohibition of Chemical and Biological Weapons (Prohibition of Chemical and Biological Weapons Act), Law no. 11 690 as amended up to 23 Mar. 2013, <<http://www.law.go.kr/lsInfoP.do?lsiSeq=137009&efYd=20130323>> (in Korean). In addition, transactions with North Korea are regulated by the Ministry of Unification, under the Inter-Korean Exchange and Cooperation Act. Transactions with North Korea are not recognised as import or export; instead, the terms 'taking in' and 'taking out' are used. 27 Public Notice on Trade of Strategic Goods and Technologies, Ministry
- ² Public Notice on Trade of Strategic Goods and Technologies, Ministry of Trade, Industry and Energy Notice no. 2013-39, 31 March 2013, <<http://law.go>
- ³ Public Notice on Trade of Strategic Goods and Technologies (note 27), Article 1.2
- ⁴ Public Notice on Trade of Strategic Goods and Technologies (note 27), Annex 4 (controlled items categorised by the multilateral export control regimes and treaties); Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Biological and Toxin Weapons Convention, BTWC), opened for signature 10 April 1972, entered into force 26 March 1975, United Nations Treaty Series, vol. 1015 (1976); and Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention, CWC), opened for signature 13 January 1993
- ⁵ Korea Strategic Trade Institute (KOSTI) and Korea Institute of Nuclear Nonproliferation and Control (KINAC), [Atomic export control guide] (KOSTI/KINAC: Seoul, Nov. 2011), <<https://www.kosti.or.kr/kosti/downloadAction.do?fileName=1849>> (in Korean), p. 13
- ⁶ Foreign Trade Act (note 26), Article 19(1)
- ⁷ Defense Acquisition Program Act (note 26), Article 34
- ⁸ These 12 categories are: (a) firearms and other fire power weapons; (b) guided weapons; (c) aircraft; (d) vessels; (e) ammunition; (f) tanks, armoured vehicles and other mobile combat equipment; (g) radars, friend or foe identification devices, and other communication and electronic equipment; (h) night observation devices and other optical or thermal imaging devices; (i) combat engineering equipment; (j) chemical, biological and radiological warfare equipment; (k) command and control systems; (l) other materials that the head of the Defense Acquisition Program Administration designates as recognised to be important for military strategy or tactical operations. Defense Acquisition Program Act (note 26), Article 35(2)
- ⁹ Presidential Decree no. 24 442 on the Defense Acquisition Program Act, 23 Mar. 2013 <<http://www.law.go.kr/lsInfoP.do?lsiSeq=136012>> (in Korean), Article 39(2)
- ¹⁰ Public Notice on Trade of Strategic Goods and Technologies (note 27), Article 4
- ¹¹ Yestrade, <<http://www.yestrade.go.kr/>>
- ¹² Applications can be submitted online via the Defense Trade Service website, <<http://www.d4b.go.kr/>>
- ¹³ Wetter, A., Enforcing European Union Law on Exports of Dual-Use Goods, SIPRI Research Report no. 24 (Oxford University Press: Oxford, 2009), p. 67
- ¹⁴ Korea Strategic Trade Institute (KOSTI), [Annual report 2011] (KOSTI: Seoul, 2011), p. 109 (in Korean)
- ¹⁵ <http://www.yestrade.go.kr/portl/jsp/si/sposi050lf.jsp> (in Korean)

for the increasing demands of enhanced export controls.

As a result, the Foreign Trade Act was amended in September 2003 to create an online system, subsequently named Yestrade, for the management of strategic items. In 2007 the Foreign Trade Act was fully amended and export controls on strategic items were strengthened more generally.

For example, the Korea Strategic Trade Institute ('KOSTI') was established to support the implementation of export controls, including activities such as identification services.

The South Korean government has continuously amended its provisions on export control in order to reflect changes in the multilateral export control regimes and has developed ever more sophisticated legal instruments, always bearing in mind the need for a

balance between export promotion and non-proliferation.

Between 2004 and February 2013 the Public Notice on Trade of Strategic Goods and Technologies – which lists the items subject to export control – was amended 15 times. Until 2009 the list was updated irregularly; since then, the authorities have updated it at the end of each year to reflect changes in the control lists of the multilateral export control regimes. While most of the amendments to the Public Notice have dealt with the annual updates to the lists of the four regimes, provisions for transit and transshipment and brokering licences have also been added. In addition, exceptions have been added to the 'catch-all' clause, which requires exporters to obtain export permits for items not mentioned in control lists but which may be

intended for use in a WMD programme.

In addition, the Denial List – which lists end-users for whom exporters are requested to contact the licensing authorities to obtain catch-all licences – has been reduced from around 7,000 to around 600 individuals and companies¹⁵

The larger Denial List was based on lists from the UN Security Council's lists of denied parties and the four export control regimes' licence denials. The shorter amended list now follows the UN Security Council's designation. The South Korean government has not required the import of dual-use items to be reported since November 2009.

A further amendment to the Foreign Trade Act was passed in 2013 and came into force on 30 January 2014. The amendment makes several changes to support legal trade flows. For example, it expanded the scope of items for identification by KOSTI – exporters can apply for the identification of items designated by the government in consideration with catch-all clauses, meaning a company can potentially reduce the risk of an illegal export caused by its subjective judgement on identification of items to be exported.

The amendment also obliges traders to obtain brokering licences for catch-all clauses. In addition, universities and research institutes now can obtain certification of having an internal compliance programme in place. Furthermore, the government is currently addressing issues regarding conflicting definitions between the munitions list (annex 3) and defence industry materials. With the amendment to the Foreign Trade Act, export licences are exempted when traders obtain permits from DAPA. The government is also in the process of amending the Defense Acquisition Program Act to support this change.

This article is an edited and updated version of one first published by SIPRI in June 2013.

(<http://books.sipri.org/files/misc/SIPRIBP1311.pdf>)

Jaewon Lee is a researcher with the Science and Technology Policy Institute, Sejong, Korea. writejaewon@gmail.com

State Department releases military drone export guidance



In February, the U.S. State Department released a fact sheet describing its policy on the licensing and export of military and commercial unmanned aerial systems (drones). Reid Whitten examines the policy and its implications in an extremely competitive international marketplace.

The United States has a responsibility, or so the State Department tells us, to ensure the sales and exports of unmanned aerial systems ('UAS') are consistent with U.S. national security interests, U.S. policy, and even U.S. values. While the government would be glad to keep the export of military drones in lock-step with our policy goals, the realities of a rapidly expanding UAS market and global competition has forced export regulators to consider how to balance the potential loss of economic opportunity against the loss of control of UAS technology.

On 17 February, the State Department released a fact sheet describing its new policy (the official policy is classified) on licensing the export of military and commercial drones. From what we can see, the regulators have declined to significantly unclench restrictions on drone exports. Drone export licence applications will be considered on a 'case-by-case' basis. Although a case-by-case assessment does leave room for manufacturers to hope that they will be

allowed to begin exporting drones, without a broader authorisation, the bureaucratic process of acquiring a licence for every transaction may

From what we can see, the regulators have declined to significantly unclench restrictions on drone exports.

hinder U.S. manufacturers in competing in the world market.

The problem with regulations in this area is that the United States does not hold as clear a competitive advantage in drone production as it does in heavier military manufacturing. Currently, China and Israel lead the pack in the \$6 billion drone market, positioning themselves ahead of the United States because of the limitations on U.S. exports. In addition, countries including India, Iran, Russia, Taiwan, Turkey, and the United Arab Emirates are also

developing drones. Although the United States will be reigning in the sales of Predators, Reapers, and Global Hawks, by maintaining strict licensing requirements for export, China, notoriously less scrupulous about selling arms to the highest bidders, may be making similar technologies available to all comers. The conditions placed on the export of military UAS will reportedly include:

- Sales and transfers of sensitive systems to be made through the government-to-government Foreign Military Sales programme;
- Review of potential transfers to be made through the Department of Defense Technology Security and Foreign Disclosure processes;
- Each recipient nation to be required to agree to end-use assurances as a condition of sale or transfer;
- End-use monitoring and potential additional security conditions to be required; and
- All sales and transfers to include agreement to principles for proper use.



The last condition appears to be an attempt to preempt the loud and growing objections, both at home and abroad, to the use of drones. Those opposed to or hesitant over the military use of drones note that drones may be used, intentionally or unintentionally, by a government to harm innocent civilians or violate human rights. In apparent response to those objections, the State Department lists the following principles to which end-users of drones must agree:

- Recipients are to use these systems in accordance with international law, including international humanitarian law and international human rights law, as applicable;
- Armed and other advanced UAS are to be used in operations involving the use of force only when there is a lawful basis for use of force under international law, such as national self-defence;
- Recipients are not to use military

Links and notes

The fact sheet is at:
www.state.gov/r/pa/prs/ps/2015/02/237541.htm

UAS to conduct unlawful surveillance or use unlawful force against their domestic populations; and

- As appropriate, recipients shall provide UAS operators technical and doctrinal training on the use of these systems to reduce the risk of unintended injury or damage.

Interestingly, the new export policy follows on the heels of an announcement by the Federal Aviation Administration of new regulations related to the use of drones domestically. The FAA rules permit domestic use of UAS under certain specific conditions, including:

- UAS must weigh less than 55 pounds;
- UAS must be limited to an airspeed of 100 mph and an altitude of 500 feet;
- UAS may be flown only within sight of the operator; and
- UAS may only be flown by persons certified by the FAA.

The regulation of drones, both for domestic use and for export, is a

complicated task for any one agency, let alone a number of agencies attempting to coordinate between their bureaucratic processes. However, no matter how lumbering and lurching efforts at regulation may appear in comparison with the rapid and constant developments in drone technology and use, government regulators are working constantly to define their stance on the manufacture, sale, and operation of UAS. It follows that the regulations will be subject to sudden change over the coming years. Companies seeking to position themselves in the burgeoning drone market would be well advised to remain on top of the applicable regulations.

Reid Whitten is an international trade associate in Sheppard Mullin's Government Contracts, Investigations & International Trade Practice Group in the firm's Brussels and Washington, D.C. offices

rwhitten@sheppardmullin.com

grayston & company

**Your legal hub for the EU
Export Control - Sanctions
Customs - Trade**

Tel.: + 32 2 737 13 60 Fax: + 32 2 791 92 71 info@graystoncompany.com
www.graystoncompany.com

BOARDTALK



There is a tendency – within business and policy – to conflate export controls and sanctions practice – and for good reason, in the sense that many of the procedures required for compliance (screening, due diligence, understanding of products and customers) are similar, and that the policy drivers (proliferation threats, regional and international security, national interest etc.) come from the same source. But for this issue, **we asked our panel to put their finger on the key (if subtle) differences between sanctions and export control compliance.**

Jim Stearns and John Pisa-Relli, Accenture

Compliance responsibility for sanctions and export controls typically is combined in-house under a single umbrella. Accenture combines responsibility for both areas under a single Global Trade Compliance Programme in the company's legal department. Although they can be distinguished in any number of meaningful ways,

sanctions and export controls comprise various national and international legal requirements that share the common purpose of restricting cross-border activities on the basis of WHERE a company does business, WHO it does business with, and WHAT industries and technologies are involved.

Despite this common purpose, there are practical differences to approaching each area that bear mention. For

example, sanctions are more likely to be imposed rapidly in response to ever-changing world events. In contrast, export controls are often imposed following a more deliberate process, as shown by the Obama Administration's multi-year export control reform efforts. Consequently, sanctions may take a company by surprise and have a disruptive impact whereas export controls often follow a notice and

The Board



Lillian Norwood, IBM

Lillian Norwood is a Manager for IBM's Export Regulation Office. She has responsibility to ensure export regulation compliance with a

focus on technology transfer, which has a large impact across multiple IBM organisations including Engineering, Manufacturing, Research, and Systems & Technology Group. She also has managerial responsibility for export compliance within IBM's Global Service engagements, patents, external relationships and anti-boycott compliance. Lastly, she has oversight of IBM's internal export education programme and performs compliance reviews of IBM's worldwide export network. The activities associated with these responsibilities include: regulation interpretation; classification of technology, software and hardware; deemed export processes; cloud export requirements; due diligence for acquisitions and divestitures; oversight, planning and delivery of worldwide export education seminars; and interfacing with government officials to ensure the necessary export authorisations are obtained for technology transfers.



Fredrik Hallgren, Ericsson

Fredrik is the Director of Group Trade Compliance (Group Function Legal Affairs) responsible for the trade compliance programme within

the Ericsson Group. As such, it is his responsibility to ensure that the Ericsson Group is well equipped to comply with export controls, sanctions and customs regulations worldwide. This includes governance, steering documents, processes and procedures, IT tools and audits.



John Pisa-Relli, Accenture

John is the managing director of trade compliance for Accenture, a \$30+ billion consulting, technology, and outsourcing company with more than

300,000 employees in over 50 countries.

In this role, he leads the company's internal trade compliance programme and legal team, and serves as chief in-house counsel on all matters pertaining to

economic sanctions, export controls, and other legal requirements that impose restrictions on the worldwide transfer of goods, technology, and services.

Prior to joining Accenture, John served in the U.S. federal government, practised law privately, and served as in-house legal director for trade compliance with Thales, a multinational aerospace and defence company headquartered in Europe.

The views expressed in this article do not necessarily represent those of his employer or any other third-party.

John welcomes your feedback and can be reached at john.c.pisa-relli@accenture.com.



Jim Stearns, Accenture

Jim is the Director of Legal Services, Trade Compliance (Americas) for Accenture LLP, handling economic sanctions and export control

issues for the company. Prior to joining Accenture, he headed Intelsat Corporation's trade compliance team. Jim had a 20-year career in private practice before entering the corporate sector and also served in several U.S. government agencies, including the Department of Commerce.

comment process that allows for a company to anticipate and react in a more thoughtful manner. Also, sanctions generally resonate more effectively with company personnel than export controls. Any employee is likely to understand, from news reports if nothing else, that Iran is off limits because of international sanctions driven by concerns over support for terrorism. Conversely, complex export control restrictions on the cross-border transfer of data encryption technology may be inscrutable to all but the savviest subject matter expert.

However, practical differences ultimately are the realm of subject matter experts, and compliance will be weakened if the average employee does not understand basic requirements of sanctions and export controls. In this connection, Accenture took stock of its own global trade compliance programme and consolidated previously separate sanctions and export control compliance policies into one simple and clear international trade controls policy based on the WHERE, WHO, and WHAT principles. This unified approach dramatically improved awareness and

comprehension of these complex legal areas, and helped company personnel at all levels of sophistication and responsibility better learn to spot and

Compliance will be weakened if the average employee does not understand basic requirements of sanctions and export controls.

escalate sanctions and export control issues, leaving the nuances to internal subject matter experts.

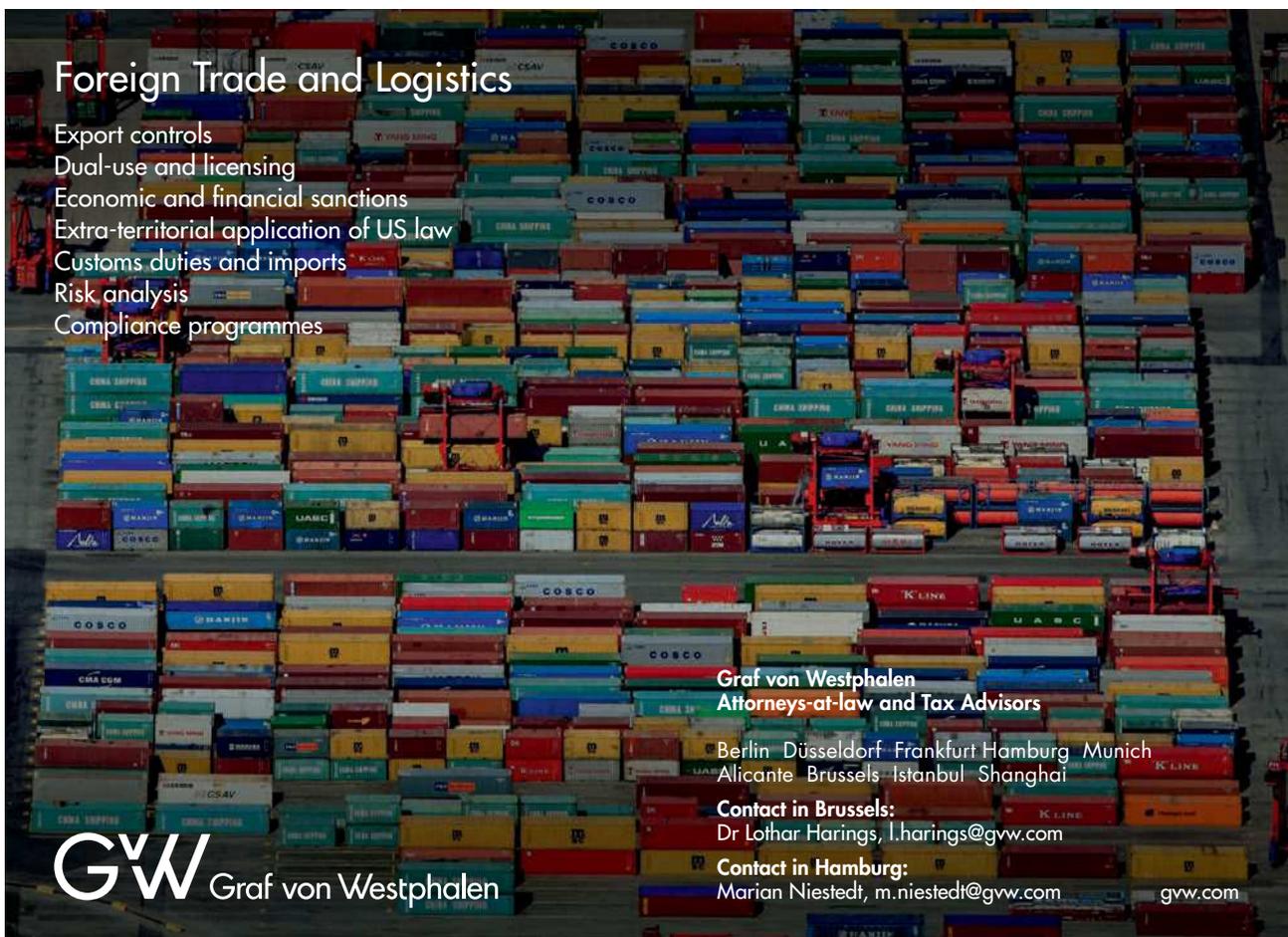
Lillian Norwood, IBM

For my company, the compliance requirements for both export controls and sanctions are managed centrally within the corporate headquarters' export regulation function. The compliance programmes which have been implemented must be responsive to changing environments, whether that be different business requirements or regulatory changes – including

sanctions which may come at a moment's notice. The difference would potentially be in the determination on which areas (if any) under the compliance programme are affected by the modified sanctions versus having to make an overall change to the programme.

Fredrik Hallgren, Ericsson

From an in-house perspective there is quite a difference between export controls and sanctions. Obviously there is a difference in that export controls usually involve some kind of authorisation procedure with export licences whereas sanctions are usually more black and white with prohibitions. For this reason it is possible to have a dialogue with a licensing authority but you are left more on your own with your sanctions screening. Also, the nature of the export control legislation is that it's predictable and only changes over mostly long cycles. Sanctions are much more reactive in nature and could change substantially overnight. This makes the sanctions legislation much more challenging to deal with from an operational perspective.



Foreign Trade and Logistics

- Export controls
- Dual-use and licensing
- Economic and financial sanctions
- Extra-territorial application of US law
- Customs duties and imports
- Risk analysis
- Compliance programmes

Graf von Westphalen
Attorneys-at-law and Tax Advisors

Berlin Düsseldorf Frankfurt Hamburg Munich
Alicante Brussels Istanbul Shanghai

Contact in Brussels:
Dr Lothar Harings, l.harings@gvw.com

Contact in Hamburg:
Marian Niestedt, m.niestedt@gvw.com

gvw.com

GW Graf von Westphalen

Israeli sanctions: difficult – but not impossible – to navigate



Tougher trade sanctions and a shortage of practical guidance from Israel's regulatory authorities, makes compliance with the country's trade regulations difficult, but not impossible, writes Doron Hindin.

The year 2014 saw some big-name institutions hit the headlines for being brought to book for breaches of U.S. sanctions, with BNP Paribas's \$9 billion fine representing a landmark in sanctions enforcement. But it isn't only U.S. agencies that are on the lookout for sanctions violators. Israeli authorities, for one, are likewise on the prowl for their own 'BNP Paribas'. With that in mind, the following is a review of current Israeli sanctions law and related developments.

Iran springboards sanctions reform

Israel's stern foreign policies on Iran have been attracting increasing world attention. One mostly underpublicised manifestation of these policies lies within Israel's recently reformed trade sanctions regimes. Specifically, the Law on the Struggle Against Iran's Nuclear Program has significantly broadened Israel's sanctions programmes. Moreover, following new Iranian sanctions regulations passed in March 2014, the nascent 'Sanctions Bureau' within the Israeli Ministry of Finance sprang into action. As described by its leadership, the Sanctions Bureau will serve as a focal point for all sanctions-related matters, from the listing and delisting of proscribed entities to spearheading interdepartmental information exchange. What this means for businesses is that there is now a centralised Israeli governmental body responsible for coordinating enforcement activities and for actuating criminal prosecutions and convictions.

The amended ordinance

The legislation and formation of the Sanctions Bureau are all part of Israel's bolstering of its Iranian sanctions programme. However, the reforms reach far beyond trade with Iran – the

Iranian sanctions laws have brought about critical amendments to the 1939 Trading with the Enemy Ordinance ('the Ordinance'), Israel's central sanctions legislation that bans trade with all enemy states and entities (and not just those related to Iran). Accordingly, the Ordinance has been amended so that prison sentences for violations are increased from seven to ten years; harsh monetary penalties have been established; select UN Security Council sanctions have been

The topic of Iranian sanctions has given Israeli authorities a context within which to direct businesses to adopt risk-based compliance mechanisms that go far beyond domestic laws.

adopted; violations of the Ordinance have been classified as 'Original Offenses' under Israel's anti-money laundering laws; and strict new reporting obligations have been instituted (specifically, reports must now be filed with the Israeli police every time a request is received for a transaction that could violate the Ordinance).

Foreign sanctions law in Israel

Interestingly, the topic of Iranian sanctions has given Israeli authorities a context within which to direct businesses to adopt risk-based compliance mechanisms that go far beyond domestic laws. Thus, banks, credit institutions, and companies subject to Israeli securities regulations have been issued directives by the Supervisor of Banks and by the

Chairman of the Israeli Stock Exchange mandating risk analyses and reporting mechanisms that incorporate U.S., EU and UN Security Council sanctions programmes. These programmes ban trade with hundreds of individuals and entities that are otherwise not subject to Israeli sanctions.

Compliance pitfalls

Despite the recent sanctions reforms, and in spite of the clear motivations of Israeli authorities towards enforcement, the entire sanctions system remains difficult to navigate. The confusion stems first and foremost from a systemic lack of guidance by the relevant Israeli regulatory authorities. To further confound exporters, Lebanon, a country subject to a comprehensive Israeli trade ban, is a perfectly valid trading partner under U.S. and EU laws (this inconsistency often raises difficulties for companies with nexuses to both Israel and the U.S. or EU).

As a result of these factors, unanswered questions abound that constantly aggravate compliance efforts. For example: What is the liability of an Israeli entity whose products are inadvertently exported to a sanctioned country through an innocent third party? What compliance measures are expected from businesses to prevent this from happening? To what extent are Israeli parent companies or beneficiaries liable for activities of their foreign entities (especially when the foreign entity is acting in compliance with its applicable law)? Must websites block access and deny service to residents of sanctioned states? Are KYC (know-your-customer) procedures for anti-money laundering compliance sufficient for sanctions purposes? How do foreign-listed Israeli companies remain compliant with Israeli sanctions laws, and to what extent are these measures more demanding for private equity funds? What protections exist for those required to report suspicious sanctions-related transactions or for 'whistle blowers'? How does one go about obtaining an exemption for exports of medicines, religious articles, or humanitarian aid? And what if one

intends to export online tools that facilitate access to information and freedom of expression?

These unanswered questions lead to a perplexing export system under Israeli sanctions laws. While it is true that we cannot reasonably expect Israeli legislation and regulators to address the endless questions that arise with respect to sanctions laws, the complete absence of regulatory guidance has profoundly frustrated Israeli exporting efforts. At the same time, and in spite of the endless uncertainties, the recent reforms indicate that authorities are preparing to investigate and penalise sanctions evaders. The combination of these two factors – a lack of regulatory guidance coupled with increased enforcement activities – has led to a precarious trade landscape in Israel.

Hedging and risk management

To mitigate risks in the face of such confusion, companies with an Israeli nexus have increasingly adopted stricter and more robust trade policies and procedures. They have similarly armed themselves with legal memoranda and opinions and, sometimes, even with semi-formal 'pre-rulings' or 'quasi-licences' from

While it is true that we cannot reasonably expect Israeli legislation and regulators to address the endless questions that arise with respect to sanctions laws, the complete absence of regulatory guidance has profoundly frustrated Israeli exporting efforts.

the relevant Israeli government ministries. It is the hope that such measures will both help prevent compliance breakdowns as well as insulate companies and senior management in the event that these breakdowns nevertheless occur.

While the \$9 billion BNP Paribas fine is significantly higher than what we can expect from any Israeli action, the recent amendments to sanctions legislation, the newly operational

Corporate structures and indirect trade

The outdated Ordinance broadly prohibits both direct and indirect trade, but fails to adequately address a number of questions related to corporate structures and ownership. For example, there is no clarity regarding whether the Ordinance applies to conduct of foreign subsidiaries of Israeli companies. To what extent are Israeli ultimate beneficial owners liable for the activities of foreign entities?

Conversely, tough questions arise when sanctioned persons purchase

securities of Israeli companies, a likely occurrence for Israeli companies listed on foreign stock exchanges. In such cases, can the Israeli companies make capital distributions knowing that funds may ultimately arrive in the hands of residents of enemy states?

These and other questions frequently arise especially with respect to Lebanon, a country subject to a complete Israeli trade ban, but with which trade is entirely permitted under U.S. and EU laws.

Sanctions Bureau, and the country's increasingly resolute policies towards Iran and other embargoed countries all warrant enhanced and more sophisticated compliance efforts.

Recent reforms show an invigorated Israeli government that appears to be preparing to enforce its sanctions laws. However, companies who are facing complex legal questions have yet to receive any regulatory guidance from these authorities.

Diffuse lists

Despite the formation of the Sanctions Bureau within the Ministry of Finance, there is still no centralised body responsible for publishing lists of 'proscribed entities'. Unlike the U.S. 'SDN List' and the consolidated lists of the EU and the UN Security Council, there is no user-friendly resource in Israel through which to access a full list of sanctioned or unlawful entities. In fact, the Sanctions Bureau makes this point abundantly clear through a caveat on its website, according to which lists related to terrorist financing or money laundering are excluded from its purview. As a consequence, the average individual would have a prohibitively difficult time trying to identify the hundreds of 'unlawful associations' and 'terrorist entities' so designated under dispersed terrorism and anti-money laundering legislation.

As a recent example, Al-Shabaab was just designated by the Israeli government's Cabinet Secretary as a terrorist organisation, pursuant to the Prohibition of Financing Terrorism Law, 5765 – 2005. The designation is not published as part of any consolidated list, and locating the particular designation in Israel's

Official Gazette, even with the aid of computerised search tools, is like finding a needle in a haystack.

No licensing regime

Another daunting feature of Israel's sanctions laws is the lack of statutory exemptions or licensing processes. The 1939 Trading with the Enemy Ordinance, adopted by Israel from British WWII legislation, provides none of the exemptions that are typical of more modern sanctions laws (such as exemptions for export of medicines, religious articles, humanitarian aid, etc.). Instead, the law categorically and comprehensively bans all forms of trade, while simultaneously assigning the Israeli Minister of Finance broad powers to administer the law. What has developed in practice is a highly informal process of requesting ad hoc exemptions for transactions that would otherwise be unlawful under the Ordinance. While the Minister of Finance is prepared to issue such exemptions in appropriate cases, exporters are justifiably frustrated by this process's complete lack of procedure, transparency, or certainty.

Liability for third parties

The Ordinance fails to provide clarity as to what liability an Israeli entity would have if products are inadvertently exported to an enemy country through an innocent third party. Moreover, to date, no guidance has been offered by Israeli authorities as to what measures are expected to be undertaken by businesses to ensure that their entire incoming and outgoing supply chains are free from products or services from sanctioned countries or entities.

Vague reporting obligations

The Ordinance now requires a company or individual to report to the Israeli police any requests received for trade that can reasonably be expected

Tough questions arise when sanctioned persons purchase securities of Israeli companies, a likely occurrence for Israeli companies listed on foreign stock exchanges.

to have directly or indirectly come from enemies or enemy states. Similarly, if suspicion arises that any past transaction directly or indirectly involved an enemy or enemy state, one must similarly report such event, provided one became aware of the suspicion within six months of the suspected transaction. Failure to comply with these reporting obligations can lead to imprisonment or fines.

To its credit, the Ordinance establishes ‘whistle-blowing’ measures to preserve the anonymity of reporters and to prevent the reported materials from serving as evidence in criminal proceedings. However, there is no designated unit within the Israeli police responsible for receiving these reports and there are no established mechanisms to ensure that the statutory protections for the reporters are preserved in practice.

The online marketplace

The number and reach of Israeli e-commerce companies has grown exponentially in recent years; in contrast, Israeli sanctions laws have remained stagnant. As a result, internet companies have received no guidance as to what is expected of them by way of preventing sanctioned entities from accessing their websites or from utilising their online products or services. Are companies expected to install automated identification systems on their servers and deny access from sanctioned regions? Are know-your-customer procedures under anti-money laundering regulations sufficient for sanctions purposes? In

short, the advent and proliferation of e-commerce has given rise to novel questions of sanctions compliance.

Conclusion

The above challenges, and many others like them, have greatly dismayed exporters. Lacking regulatory guidance, and with no ‘quick fixes’ available, companies have begun developing robust trade policies and have armed themselves with legal memoranda, opinions and sometimes even with ‘pre-rulings’ or ‘quasi-licences’ from the relevant Israeli government ministries. It is hoped that such measures will adequately help companies navigate the ambiguities of Israel’s trade sanctions system and prevent (or at least mitigate) costly compliance violations.

Based in Tel Aviv, Doron Hindin is a member of Herzog Fox & Neeman's Public International Law, Administrative Law and Defense, Aerospace and Homeland Security departments.
hindind@hfn.co.il

*A new horizon
for Global
Trade
Management*



Trade Compliance	Global Trade Content	Supply Chain Visibility	Restricted Party Screening	Free Trade Agreements	Trade On-Demand
------------------	----------------------	-------------------------	----------------------------	-----------------------	-----------------

Amber Road provides a single platform that plans and executes all aspects of global trade. By enabling companies to take a holistic, integrated approach to global trade, Amber Road accelerates the movement of goods across international borders, improves customer service and reduces global supply chain costs.

Amber Road includes deep functional capabilities across all areas of global trade – trade compliance, supply chain visibility, restricted party screening and origin management. Underpinning all of these solutions is Global Knowledge®, the most comprehensive, intelligent repository of global trade content available anywhere.



For more information, please contact us at martijnvangils@AmberRoad.com, or visit www.AmberRoad.com.

SAVE THE DATES

THE WORLDECR EXPORT CONTROLS AND SANCTIONS FORUM 2015



WASHINGTON, DC
21-22 SEPTEMBER 2015

LONDON
14-15 OCTOBER 2015

For information on sponsorship opportunities, please contact
Mark Cusick > mark.cusick@worldocr.com

IP network communications surveillance systems: deciphering Wassenaar Arrangement controls

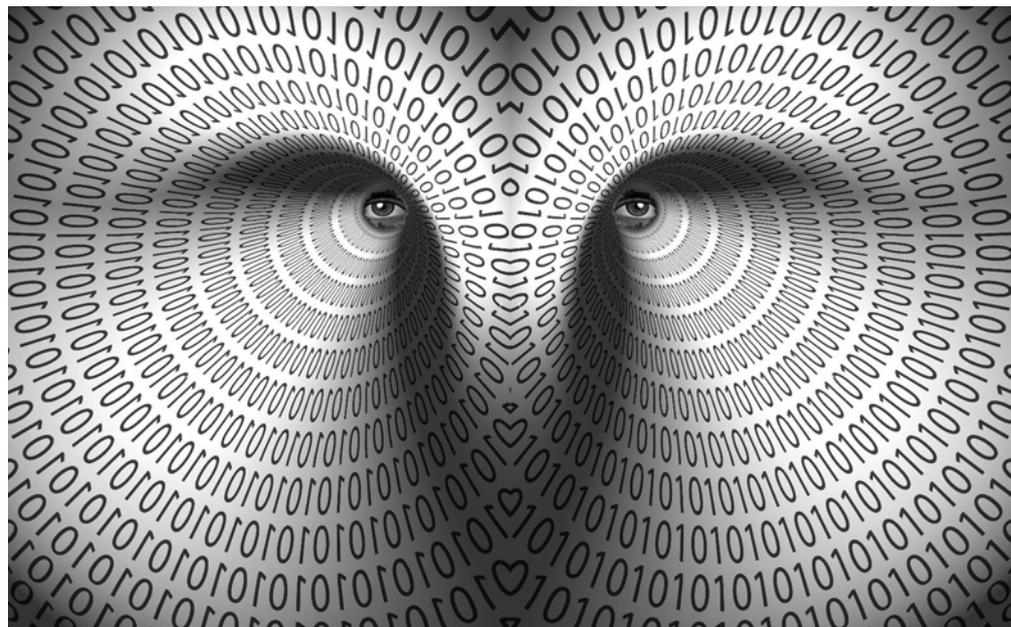
Highly technical in nature, updates to the Wassenaar Arrangement introduced at the end of last year represent the first international standard for controls on IP network communications surveillance systems. Adam Weber, Elena Hushbeck, Emily Rosenblum, Jay Johnson, Joe Petersen and Pete Heine consider their implications.

In December 2014, updates to the Wassenaar Arrangement ('WA') came into force that added Internet Protocol ('IP') network communications surveillance systems and intrusion software to the list of dual-use¹ goods and technologies to be controlled by participating governments. While these 'dual-use' systems and software can be used for commercial and national security purposes, they also raise serious security, human rights, and personal privacy concerns.

In 2011, the *Wall Street Journal* reported that since 2001, the IP surveillance technology market had grown from virtually nothing to nearly \$5 billion per year.² A report by the New America Foundation cites three key reasons for the huge growth in demand for these surveillance tools³:

- Terrorist attacks over the last decade and a half, e.g., on 11 September 2001, are often blamed on intelligence failures, emphasising the need for better intelligence-gathering capabilities.
- Technologies are generating increasingly large amounts of data, creating opportunities for law enforcement and the intelligence community but also creating challenges for regulatory and legal frameworks.
- Governments depend on commercially available tools and products.

Surveillance technologies can be used by governments to aid law enforcement and intelligence communities, and they can also be used by commercial enterprises to identify trends in market research and customer data. However, surveillance technologies can also be used by



governments to commit human rights abuses and to violate personal privacy. The advent of the Arab Spring revealed several countries (e.g., Syria and Libya) that use surveillance technologies to target their citizens for repression.⁴ Ethiopia also has a history of extensive use of telecommunications and Internet surveillance on its citizens.⁵ Ironically, countries like the United States, Germany, and the United Kingdom, which are known for promoting human rights, are responsible for the majority of surveillance technology exports abroad.⁶ Between 2003 and 2013, the German government reportedly approved licences for the export of surveillance technologies to at least 25 countries.^{7,8}

Prior to the WA controls, the legal requirements for control of these systems were unclear. Though they are inherently dual-use, a lack of explicit

export controls meant that regulation was limited to catch-all controls and individual government regulation, which led to a variance in implementation. For example, FinFisher and FinSpy intrusion software is owned by a British-German company. Since 2012, the U.K. has imposed controls on these software exports,^{9,10} but there is evidence that Germany did not regulate exports of this software at all.¹¹

The majority of literature to date focuses on the policy issues surrounding the export control of surveillance technology and intrusion detection software.¹² However, currently published literature does not adequately address or explain technical issues associated with the technology or the new export controls. The new WA controls are highly technical in nature and represent the first international standard for controls on

these systems. This article seeks to decipher the technical controls and promote better understanding of the technology and systems that may actually meet the control specifications.

Controls

The WA controls that address IP network communications surveillance systems are defined in the dual-use list ('DUL') Category 5 Part 1 – Telecommunications, section 5.A.1.j:

'IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
 - a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
 - b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
 - c. Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
 - a. Execution of searches on the basis of 'hard selectors'; and
 - b. Mapping of the relational network of an individual or of a group of people.

Note: 5.A.1.j. does not apply to systems or equipment, specially designed for any of the following: Marketing purpose; Network Quality of Service (QoS); or Quality of Experience (QoE).

Technical Note

'Hard selectors': data or set of data, related to an individual (e.g., family name, given name, e-mail, street address, phone number or group affiliations).'

Key technical definitions

IP network communications surveillance systems or equipment
These are systems that can intercept data from the network directly. The technology differs from other

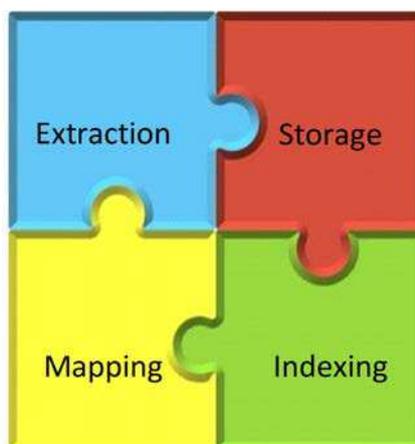


Figure 1. Core functions of IP network surveillance systems

surveillance systems such as wiretapping, where a specific phone line is tapped, or intrusion software, which targets individual computers, infecting the computer with software that allows for surveillance monitoring.

IP network communications surveillance systems target the whole network, which could be as small as the office network of a small business or as large as the entire network of a service provider like AT&T or Verizon. IP network surveillance technology can be used like wiretapping to monitor a specific user, or it can be used to monitor large numbers of users.

Carrier class IP network (e.g., national grade IP backbone)

These are the networks of the core providers. Core providers include cell phone service providers and Internet service providers. Some are well known, such as AT&T and Sprint, but there are other less recognisable core providers that also manage the networks and the distribution of information on the back end of the system. Systems that are capable of tapping into networks can intercept all of the data transmitted on those networks.

For a small internal network at a small business, the systems can intercept all information employees send over the network. For a large backbone network, the systems can intercept all information, such as the billions of phone calls and emails that people send over that network every day. By including language specifying carrier class IP networks, the WA controls are only targeting the systems capable of intercepting the largest amounts of data.

Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection [OSI] model [ISO/IEC 7498-1])

The application layer is the layer of information that is in 'human language', as opposed to 'computer language'. Applications include, among many other things, emails, website visits, documents, photos, movies, chat messages, and social media. The application layer is known as layer 7 of the OSI model,¹³ the model commonly used to describe network communications.

Core functions of IP network surveillance systems

Network surveillance comprises four core functions: extraction, storage, indexing, and mapping (Figure 1).

Extraction

Extracting the data from the network is the most important function of an IP network surveillance system (Figure 1). If the system lacks the ability to intercept and extract the data from the network, then the rest of the functions are somewhat irrelevant, and it will have nothing to store, index, and analyse. The amount of data that the system is able to extract is also crucial. These systems must be capable of dealing with petabytes (millions of gigabytes) of data. The carrier grade

IP network surveillance technology can be used like wiretapping to monitor a specific user, or it can be used to monitor large numbers of users.

networks of the backbone carry and transmit the data of millions of users every day. There are a number of systems that are already designed to do this. These systems typically come from network vendors, and are typically oriented towards support for law enforcement interception of data.

The Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP) to route data from its source to its destination. Data is packaged and sent in individual packets comprising two components, the header information and the data payload. The header information contains the source

and destination addresses. The data payload contains the layer 7 application data (e.g., emails and documents). A single document or email may be divided into multiple packets and routed separately over the Internet using the fastest path, and reassembled for delivery to the user. Deep packet inspection is necessary to read and re-assemble the payload data of the packets.

The data-extraction process begins by obtaining a copy of the network traffic packets as they are sent through the network. This is usually done using a network tap, which can be an electronic device that passively copies the data or a fibre-optic splitter that mirrors the light passing through fibre optic cable, creating a duplicate signal. In both cases, as network traffic passes through the tap, a copy is sent to a third party. Typically, network taps are not detectable and will not affect the network communications between the sender and receiver.

Another option for monitoring network traffic is port mirroring, an option available on many switches and routers. Port mirroring uses software to actively capture network traffic of interest and send an additional copy to a monitoring device. Using port mirroring for large-scale surveillance can decrease the performance of the network device, causing packets to be dropped randomly due to overload, and can diminish overall processing power.

Copying and capturing every network packet on a massive scale is unrealistic. Rather, it is more common to monitor specific network connections. If the user's unique IP address is known, it is possible to capture network traffic that matches the intended destination while excluding other traffic from the capture. Modern network taps and port mirroring devices can selectively filter network traffic being copied. Monitoring software capable of deep packet inspection may also have the ability to selectively capture the traffic of interest.

Storage

Another core function of the network surveillance process (Figure 1) is storing the extracted data. Storage can occur throughout the process, including storage of the raw data from the network taps as well as the re-assembled data. Storing the data is a

relatively simple function because large-data storage hardware is very common and has dropped in price over the years. However, there are often practical limits on how much captured network traffic can be realistically stored, even with massive storage systems. These limits may affect the volume of network traffic stored and how long that data can be stored before being overwritten. While storage is required for indexing and analysis, the

Port mirroring uses software to actively capture network traffic of interest and send an additional copy to a monitoring device.

surveillance system itself does not need to contain the storage hardware. The storage hardware can be obtained separately and connected to the surveillance system as a separate module. It is also unnecessary to have one piece of hardware capable of storing all of the data; multiple large-capacity storage hardware components could be used.

Indexing

Once the extracted data has been stored, the system needs to sort and index the data (Figure 1). As with storage, a plethora of systems exist that are very efficient at searching and indexing massive sets of data. The term 'big data' applies to data sets that are too large for traditional database indexing techniques. Parallel

processing is commonly employed to distribute indexing of big data across multiple processors and computers. Many artificial intelligence concepts may be used in such systems for efficient searching. Many sectors of industry use such indexing systems to create consumer profiles from shopper data and to identify trends in consumer purchasing across demographic groups.

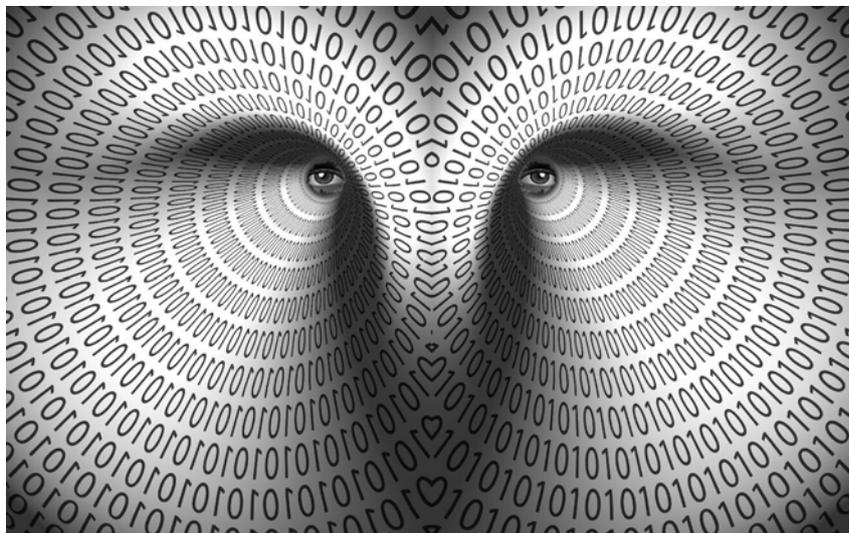
Mapping

Once the data has been sorted and indexed, it is mapped to create relational networks of an individual or group (Figure 1). Mapping the data identifies and analyses the connections between individuals or groups by using hard selectors such as names, email addresses, phone numbers, locations visited, products bought, and group affiliations. Creating relational networks allows a user to organise and provide context for the data that has been extracted and indexed.

Exceptions to controls in section 5.A.1.j

These controls contain a note that lists three exceptions for systems and equipment that are specially designed for marketing purposes, ensuring network quality of service ('QoS'), and ensuring quality of experience ('QoE').

The first exception is systems specially designed for marketing purposes. Companies want to know what individuals and groups purchase, and they use these systems to comb through millions of consumer purchases to identify overarching trends, as well as to create individual buying profiles. This information is



then used by marketing offices to help tailor shopping experiences to the consumer in order to better target customers with promotions and advertisements. This targeting can range from the innocuous – having Netflix suggest a new show to watch on the basis of past preferences – to the more troubling, where Target utilised a customer's Guest ID number (tied to credit card, name, and email address) to determine that she was pregnant even before her family knew.¹⁴

The second and third exceptions, ensuring network QoS and QoE, are similar to each other. These exceptions refer to systems that monitor network traffic behind the scenes. QoS systems may use deep packet inspection to examine network traffic flows in order to ensure smooth traffic, and can interface with other network systems to reroute traffic on the network when certain pathways are experiencing high loads.

QoE systems are similar to QoS systems, but they monitor the user experience instead of network traffic flows. They can help identify network bottlenecks due to massive file

downloads. They can also help identify traffic that can be blocked, such as copyrighted materials being downloaded on peer-to-peer file-sharing networks. In most cases, this

Individual systems, which are not controlled, could be used in aggregate to create a system capable of performing all of the functions listed in the controls.

sort of software has been designed to not allow identification of traffic tied to a specific individual or group, so that these solutions cannot be used for surveillance purposes.

Potential problems

From a technical perspective, there are two potentially serious issues with the controls of 5.A.1.j.

First, the control language states

that all requirements must be met for a system to be controlled. However, there are currently a very limited number of systems that perform all of the required functions. Many smaller systems can perform one or two of the core functions very well. As mentioned above, both large-data storage hardware and big-data/large-database indexing and searching tools are quite common. Deep packet inspection systems are also commonly used in modern network intrusion detection and prevention systems and data-loss prevention systems in order to detect malicious network traffic and unsanctioned file transfers. Network extraction systems are less common, but also exist. Individual systems, which are not controlled, could be used in aggregate to create a system capable of performing all of the functions listed in the controls. This could potentially be an easy way to bypass the controls.

The second potentially serious concern is the exception for systems specially designed for marketing purposes. Specially designed systems for marketing purposes can, from a technical standpoint, be virtually

Fried Frank

No Borders, Know Boundaries

As trusted advisors to clients operating or investing across international borders, we are regularly called upon to provide specialist international trade and investment counsel on a wide variety of regulatory, investigative, and enforcement matters worldwide. Our practitioners draw upon a long history of senior US government and diplomatic service to deliver timely, actionable advice which combines policy acuity, deep multi-jurisdictional legal expertise, and practical business judgment. For more information about our practice and capabilities, please contact our practice leader directly in confidence:

The Hon. Mario Mancuso, Head of International Trade and Investment
Washington, DC
+1.202.639.7055
mario.mancuso@friedfrank.com



Links and notes

- ¹ Traditionally, the term 'dual-use' refers to goods that have both military and non-military applications. The inclusion of IP network surveillance systems and intrusion software on the WA Dual-Use List represents an expansion of the dual-use concept.
- ² Valentino-Devries, J., Angwin, J., and Stecklow, S., 2011, 'Document Trove Exposes Surveillance Methods.' *Wall Street Journal*. <http://www.wsj.com/news/articles/SB10001424052970203611404577044192607407780?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052970203611404577044192607407780.html> (accessed January 2015).
- ³ Maurer, T., Omanovic, E., and Wagner, B., 2014, 'Uncontrolled Global Surveillance, Updating Export Controls to the Digital Age.' New America Foundation. http://newamerica.net/sites/newamerica.net/files/policydocs/Uncontrolled_Surveillance_March_2014.pdf (accessed February 2015).
- ⁴ Ibid.
- ⁵ Human Rights Watch, 2014, 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia.' http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf (accessed February 2015).
- ⁶ Ibid
- ⁷ Countries of documented export include Albania, Argentina, Chile, India, Indonesia, Qatar, Kosovo, Kuwait, Lebanon, Malaysia, Morocco, Mexico, Norway, Oman, Pakistan, Russia, Saudi Arabia, Switzerland, Singapore, Taiwan, Turkey, Turkmenistan, the USA, and the UAE. No information was reported on the export of FinFisher to Bangladesh, Netherlands, Estonia, Australia, Mongolia, Bahrain, and Nigeria, despite evidence that the software was sold to these countries.
- ⁸ Wagner, B., and Guarnieri, C., 2014, 'Exclusive: German Companies are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions.' *Global Voices*. <http://globalvoicesonline.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/> (accessed February 2015).
- ⁹ Silver, V., 2012, 'U.K. Limits Spyware That May Have Targeted Dissidents.' *Bloomberg Business*. <http://www.bloomberg.com/news/articles/2012-09-10/spyware-matching-finfisher-can-take-over-iphones> (accessed February 2015).
- ¹⁰ Burns, C., 2012, 'UK Uses Encryption Controls to Prevent Export of FinSpy Trojan'. *Export Law Blog*. <http://www.exportlawblog.com/archives/4347> (accessed February 2015).
- ¹¹ Wagner, B., and Guarnieri, C., 2014, (See 8)
- ¹² Kehl, D., and Morgus, R., 2014, 'The Dictator's Little Helper: How to Stop Western Companies from Exporting Surveillance Technologies to Authoritarian Governments.' *Slate*. http://www.slate.com/articles/technology/future_tense/2014/03/export_controls_how_to_stop_western_companies_from_sending_surveillance.html (accessed February 2015).
- ¹³ Microsoft, n.d, 'The OSI Model's Seven Layers Defined and Functions Explained.' <http://support.microsoft.com/kb/103884>
- ¹⁴ Forbes, Kashmir Hill, 2012, 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.' February 16. <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

identical to systems designed for surveillance purposes. Both look at large amounts of data, both utilise hard selectors to identify and connect data to individuals and groups, and both analyze that data to create relational networks. The main difference at the moment is that these marketing systems typically look at data already available to the company (purchasing data, store visits, website page views) rather than extracting data from the network. Marketing systems that perform all of the core functions except for extracting data from the network are used extensively throughout legitimate enterprise.

Intrusion software and encryption

In addition to the controls of section 5.1.A.j, the DUL WA controls other surveillance software under section 4.A.5:

Systems, equipment, and components therefor, specially designed or modified for the

generation, operation or delivery of, or communication with, 'intrusion software'.

Intrusion software is distinctly different from IP network surveillance systems, and it is important to clarify those distinctions. Intrusion software is an individual piece of software (not hardware) that covertly infiltrates a target's computer in order to spy on the activity of that specific machine. While intrusion software can be covertly installed on many different machines, installation must be accomplished on each and every machine. Additionally, intrusion software is limited to accessing traffic originating or ending at that specific machine. This is far different from the systems capable of monitoring an entire network, which are controlled under section 5.1.A.j, and the two should not be equated.

Encryption

In order to prevent the interception and monitoring of sensitive network traffic with network surveillance

systems, the data packets' payload can be encrypted. Secure Sockets Layer encryption ('SSL') is typically used to encrypt traffic relating to web applications. In recent years, SSL-encrypted Internet traffic has become more common. This has created a blind spot in network intrusion detection and prevention systems and data loss prevention systems. There is a new class of devices that can decrypt SSL traffic. These products execute a 'man in the middle attack' and act as a web proxy; i.e., the device intercepts requests from the user and passes them along to the intended recipient server, but only after first decrypting and copying the data so it can be analysed.

Businesses use these products to obtain greater visibility into their own networks. These products often contain whitelists which can be used to exclude the capture of encrypted traffic from known financial or medical organisations, to comply with privacy laws. However, this same technology is being used by some governments in order to decrypt and monitor their citizens' encrypted network traffic. These devices may not be able to decrypt and re-encrypt data on a massive scale, but could be used to monitor encrypted traffic from groups of users of interest once their IP addresses are known.

Conclusion

The new WA DUL controls on IP network surveillance systems are the first international effort to regulate this growing dual-use industry. Information technology is constantly evolving and advancing, and the controls the international community uses to regulate it must evolve as well to keep pace with new advances and to address gaps and ambiguities in the controls. Understanding the technical nature of the systems is key to deciphering the controls placed upon them.

Adam Weber, Elena Hushbeck, Emily Rosenblum, Jay Johnson, Joe Petersen and Pete Heine are members of the Center for Strategic Security, Argonne National Laboratory.

<http://www.gss.anl.gov/center-for-strategic-security-overview/>

"The substance, and particularly the government and regulatory body engagement, is the most outstanding I have encountered for conferences of this type."

DIRECTOR, GLOBAL TRADE MANAGEMENT EUROPE, NORTHROP GRUMMAN



SMi group are proud to announce the 2nd

Defence Exports Asia Pacific

11th & 12th
MAY
2015

Grand Copthorne Waterfront Hotel, Singapore

*Develop Your
Export Potential*

BENEFITS OF ATTENDING:

- Assess the latest regulations in the Asian market
- Learn about individual countries' licensing procedures and international treaties
- Understand where the industry is heading and the challenges that will be faced in the future
- Engage with senior policy makers from the Asia Pacific region
- Hear from the ASEAN nations and their developments in export controls
- Hear from industry about the challenges of regional compliance

INDUSTRY SPEAKERS

 Beth Ann Johnson, Director, Global Trade Management, Northrop Grumman Corporation

 Iiyana Hristev, Director of Export and Trade Compliance, QinetiQ North America

 Harry Patel, Head of Trade Compliance, Meggitt PLC

 Julia Reed, National Director Export Controls (Australia Pacific), Airbus Group

 Lynn Parker, Regional Trade Compliance Manager, Rockwell Automation

POLICY SPEAKERS

 Jun Kazeki, Director, Security Export Control Policy Division, Ministry of Economy, Trade and Industry (METI) of the Japanese Government

 Jaeil Jo, Export Control Support Department, Korea Strategic Trade Institute

 Claire Willette, Director, Strengthening Export Controls, Australian Department of Defence

 Faizal Yusof, Deputy Director, Strategic Trade Controller, Ministry of International Trade and Industry (MITI), Malaysia

 Donald Pearce, Regional Export Control Officer, US Embassy Singapore, U.S. Department of Commerce - Bureau of Industry & Security

PLUS TWO INTERACTIVE POST-CONFERENCE WORKSHOPS I WEDNESDAY 13TH MAY 2015

A: Applying ECR in the Real World
Hosted by: Gary Stanley, President, Global Legal Services
08.45 - 12.30

B: The Definition of "Specially Designed"
Hosted by: Donald Pearce, Regional Export Control Officer,
U.S. Department of Commerce - Bureau of Industry & Security
13.00 - 17.00

Sponsored by

pillsbury

Register online at

www.defence-exportsasia.com

Alternative contact the team on +44 (0) 20 7827 6000 or email events@smi-online.co.uk



Listing dilemmas: a case study with gas control valves



Dual-use item control lists are designed to keep items which can be used for developing weapons of mass destruction out of the hands of would-be proliferators. But how easy is it to circumvent the controls by using alternative, non-controlled items? Not too difficult, suggest Elisey Andreevsky and Yury Daneykin.

Dual-use items can be used in the creation of weapons of mass destruction ('WMD'). Consequently, such items are typically subject to export control and included in control lists. But for states wishing to pursue a clandestine WMD programme, it is still possible to find unlisted alternatives to controlled items. The following (real-life) case study concerns the export of controlled dual-use gas control valves to the Islamic Republic of Iran.

Analysis of the case

This case took place in early 2011. A 31-year-old Swedish man of Iranian origin, Shabab Ghasri, had used a company in the Swedish town of Lund to export 11 very special non-corrosive valves to Iran via the United Arab Emirates. According to experts from Sweden's Agency for Non-Proliferation and Export Controls ('ISP'), these valves could be used for uranium enrichment activities.¹

Court documents show that Ghasri hadn't applied for permission to export such valves and had violated international sanctions on Iran. This apparent violation was discovered by Swedish customs officials during a random check of a shipment. According to the Swedish national broadcaster SVT, the cargo's official destination was labeled as Dubai, but it was later revealed that the final destination was to be Iran.

The Swedish customs authority contacted ISP which immediately determined that the shipment was illegal and that no export licence had been issued.

Ghasri denied criminal conduct and claimed that the valves were intended for end use in the oil and gas industry. ISP experts determined that while this was not impossible, the properties of

Reasons to include dual-use items in control lists

Reasons to include

High possibility of WMD use
Simplicity to switch the use from civil use to WMD

Reasons not to include

High utility in civil industry
High availability of item, simple manufacture

the devices, typically used in nuclear enrichment, were so advanced (and were so expensive) that there was little point in employing them for the claimed purpose.

We, the authors of this article, investigated whether it is possible to find a commonly used alternative for these valves, one not subject to export controls, not included in dual-use control lists, and not requiring any licence for export which could be used in uranium enrichment.

Determining whether to include items in dual-use control lists

There are inevitably contradictions involved in the decision as to whether a dual-use item ought or ought not be included in control lists: see 'Reasons to include dual-use items in control

lists' above. The decision whether to add a dual-use item to control lists during the lists' updating will be determined by such considerations. Nevertheless, so far as an item can be used in any WMD programme, it should remain under close attention of the exporting country.

Description of gas control valves

The control valve is one of the most common elements in any industry. It manipulates a flowing fluid, such as gas, steam, water, or chemical compounds, to keep the regulated process as close as possible within desired conditions.² Control valves are widely used in civil industry; for example, in the chemical, petrochemical, oil and gas, cryogenic, and aircraft industries, to name but a



few. But special control valves are required in facilities for uranium enrichment or in facilities that produce uranium hexafluoride (UF_6) in order to provide control of UF_6 process flow streams, while similar corrosion-resistant valves are necessary for processes in chemical weapons production.

Uranium hexafluoride is an extremely aggressive substance but it does not react with copper, nickel, aluminum, aluminum bronze, lead and Teflon. Carbon steels with low silicon content are also reasonably resistant to UF_6 , but in the presence of moisture, the resistance of such steels is reduced, especially at high temperatures.

Common civilian use

Civilian use of gas control valves is commonly seen in the oil and gas industry. In offshore projects, extracted oil is accompanied by the hydrocarbon gases associated with oil and released during its production.

DNV (Det Norske Veritas) is a classification society organised as an independent foundation with the purpose of safeguarding life, property, and the environment. In services for the energy sector (for example, supervision of oil platforms) DNV is a world leader.³

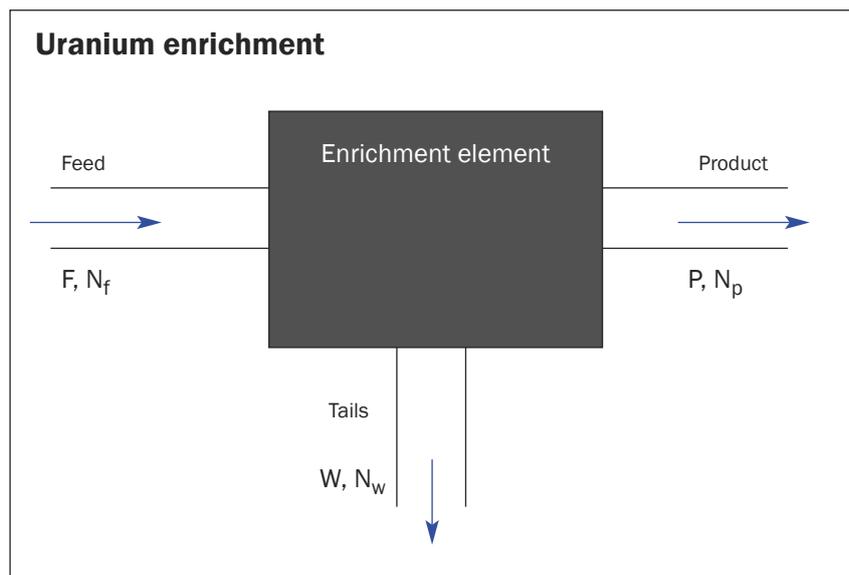
In order to understand the requirements for valves in the oil and gas industry, the authors applied the 'Offshore Standards' of DNV – ie, its standards for oil and gas processing systems. The main requirement is defined thus: design pressure shall normally include a margin above the maximum operating pressure, typically 10% and normally *minimum 3.5 bar*.⁴ This means that for the normal processing of associated gas, the valves must be able to operate with minimal gas pressure of 3.5 bar.

We chose a valve to analyse for the purposes of our study. The pressure range of the analysed valve is from 1×10^{-8} mbar to 4 bar, so it should be possible to use this valve in activities related to the oil and gas industry.

Use of gas control valves in uranium enrichment

Uranium and plutonium enrichment are the only two existing methods for producing a nuclear weapon.⁵

At present, the isotope uranium-235 is used in nuclear fuel or in nuclear weapons as fissile material, due to its



nuclear properties.⁶ The amount of this isotope in natural uranium is approximately 0.72% – this is too small a concentration for uranium-235 to be used for military or civil purposes. This creates the need for the process known as 'enrichment', the purpose of which is to separate uranium-235 from other isotopes of uranium, thus increasing the percentage of uranium-235 in the processed uranium material.

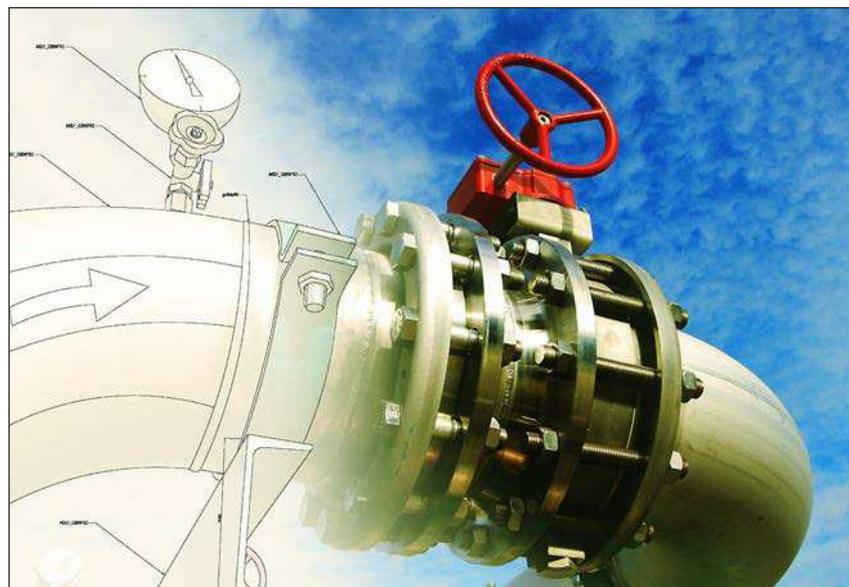
The most simplified enrichment element can be depicted as a 'black box' into which flows material with one certain isotopic composition, and out of which flow two streams with different isotopic compositions⁷ – the stream with a higher percentage of the isotope being enriched is the so-called 'product', while that with the lower

percentage of this isotope is the so-called 'tails'.

In the diagram above, 'Uranium enrichment', F, P and W stand for feed, product and tails (waste) flow rates; $N(f,p,w)$ means the percentage composition of desired isotope – ie., the number of molecules in the respective flow stream.

The number of enriching elements is arranged in a *cascade*. Those elements are arranged in 'stages' and are connected 'in parallel' (they receive identical inputs and produce identical outputs which are fed into other stages). In this way, even if one element has a small enrichment capacity, a large amount of material can be processed in a single stage.

The next step is to define the



method of isotopic separation, applied in each enrichment element.

In accordance with current uranium enrichment technologies, the authors used the gas centrifuge method of isotope separation for the purposes of this case study. In this method, gaseous uranium hexafluoride is processed inside centrifuges – rotor assemblies in which centrifugal force pushes heavier molecules to the outside of the rotor body.⁸

To understand whether the gas valves analysed in our case study could be used for pressure reduction or not, we had to determine the following parameters for a suitable valve:

- **Size:** it can be different, depending on the industrial scheme of the process. As there is a large range in sizes for most control valves, we decided to omit this parameter;
- **Pressure and temperature limits:** these parameters are dependent on the physical properties of UF₆. There is a requirement that the pressure of the UF₆ in the technological circuit must be below its sublimation vapour pressure at the operating temperature, which is usually normal room temperature ~20 °C degrees. At this temperature, the pressure of UF₆ is about 0.1 bar. This is the upper limit for pressure, because if this condition is not satisfied, the solid UF₆ will deposit on the walls of centrifuges and other technological circuits.⁹ Different centrifuge technologies may require different operating temperature and pressure, but generally these characteristics tend to the average and not increased values.
- **Construction materials,** according to the chemical properties of uranium hexafluoride. This point requires a more detailed discussion.

Control list data

A look at annex I of EC Regulation №428/2009 (position 2A226) shows which characteristics of valves are controlled in the EU. According to the annex, valves having all of the following characteristics are subject to export control:

- A 'nominal size' of 5 mm or greater;
- Having a bellows seal;
- Wholly made of or lined with aluminum, aluminum alloy, nickel,

Chemical compound of AISI 304 stainless steel	
C	max 0.08%
Cr	18-20%
Fe	66.345-74%
Mn	max 2%
Ni	8-10.5%
P	max 0.045%
S	max 0.03%
Si	max 1%

or nickel alloy containing more than 60 % nickel by weight.

(Technical Note: for valves with different inlet and outlet diameters, the 'nominal size' refers to the smallest diameter.)

As it is essential to control the gas flow, not letting it leak outside the circuit, it appears the purpose of the export controls in this case is to restrict access to the bellows (the bellows serve to create hermetic conditions required in UF₆ processing) and to the materials of the whole valve (aluminum and nickel and their alloys) – that is those to render the valve resistant to UF₆. But, having noted this, by investigating uranium chemistry, we can see that some types of stainless steel would, in theory, serve the same purpose.

Choosing appropriate materials for gas control valves in uranium enrichment

As noted above, uranium hexafluoride is a chemically active substance but it does not react with copper, nickel, aluminum bronze, lead or Teflon. Also carbon steels with low silicon content

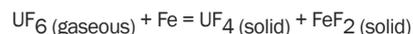
are reasonably resistant to UF₆ (but in the presence of moisture the resistance of steels is reduced, especially at high temperatures).

Let us now consider a hypothetical country which is conducting a secret nuclear programme. It is possible that it will use any appropriable equipment and technologies for that programme. So how is it likely to go about acquiring necessary items? At first instance, its choice of a suitable valve will most likely be one not on the control lists. Secondly, the process of acquiring such valve should not provoke any suspicions in the mind of the exporting company, because the exporter will have to deny the request for export (even of unlisted items) if it suspects possible military end use of this item (the catch-all principle).

With this in mind, the authors looked at classic stainless steel AISI 304. (According to the AISI¹⁰ standards on stainless steel, the chemical compound of AISI 304 stainless steel is as set out in the diagram above, 'Chemical compound of AISI 304 stainless steel'.)

The authors investigated the chemical mechanism of interactions between UF₆ and stainless steel AISI 304 and found there is a reaction between iron and UF₆, resulting in the creation of a thin iron fluoride pellicle on the surface of stainless steel.

In airless environment conditions, this reaction can be described by the following formula:



The formula shows that uranium hexafluoride forms a solid fluoride pellicle on the surface of the stainless steel that prevents further reactions; in other words, this pellicle is passivating.

The fluoride pellicle protects the

Links and notes

- ¹ <http://www.presstv.ir/detail/2012/12/04/276222/sweden-charges-man-over-iran-sanctions/>
- ² Control valve handbook // Emerson Electric Co, the USA, 2005
- ³ www.dnv.com // the official web-site of the DNV
- ⁴ "Offshore Standards" DNV-OS-E201 // The list of standards for oil and gas processing systems.
- ⁵ Alan S.Krass, Peter Boskma, Boelie Elzen, Wim A.Smit, "Uranium enrichment and nuclear weapon proliferation" // SIPRI, 1983
- ⁶ Nuclear weapon design // Federation of American scientists, 1998. www.fas.org
- ⁷ Alan S.Krass, Peter Boskma, Boelie Elzen, Wim A.Smit, "Uranium enrichment and nuclear weapon proliferation" // SIPRI, 1983
- ⁸ Gas Centrifuge Uranium Enrichment // the materials of www.globalsecurity.org
- ⁹ Alan S.Krass, Peter Boskma, Boelie Elzen, Wim A.Smit, "Uranium enrichment and nuclear weapon proliferation" // SIPRI, 1983
- ¹⁰ www.steel.org // official web-site of the American Iron and Steel Institute (AISI)

stainless steel from further interactions with UF₆, meaning that the stainless steel is, at least, an appropriate material for use in gas control valves for uranium hexafluoride processing. This stainless steel is not controlled by EC Regulation 428/2009.

Comparison of the analysed valves with the requirements for suitable valves used in uranium enrichment

Our next step was to compare the construction, pressure and temperature limits, and also the construction materials of the previously analysed valves so as to determine the suitability of certain kinds of valve for the processing of UF₆.

We looked at two valves: Valve A is an angle valve which is considered usable in uranium enrichment and subject to export control in Europe; Valve B is an angle valve commonly used in gas processing and widely used in the oil and gas industry. Valve B is not subject to export control due to its simple construction and commonly available constituent materials. (See the table 'Valve comparison'.)

Valve comparison			
	Requirements for a gas control valve for uranium enrichment	Valve A	Valve B
Temperature	~20 C	≤ 120° C	≤ 120° C
Pressure	0.1 bar	1x10 ⁻⁷ mbar to 4 bar	1x10 ⁻⁸ mbar to 4 bar
Construction materials	Cu, Ni, Al, the aluminum bronze, lead, the Teflon, stainless steel	Stainless steel or aluminum alloy	Stainless steel AISI 304L with bellows of AISI 316L (10,0-13,0% of Ni)
Status		Subject to the NPT, controlled	Not included into dual-use control lists

According to annex I of EC Regulation 428/2009 (position 2A226), valves are subject to export control procedures if only wholly made of, or lined with, aluminum, aluminum alloy, nickel, or nickel alloy containing more than 60 % nickel by weight.

In our test, we found that angle valve B could possibly be used in uranium enrichment. These valves are not subject to export control. What, then, are the repercussions in the proliferation context?

Possible scenarios

Let's return to the case of the attempted Swedish export and work through a hypothetical alternative:

Phase 1

A Swedish man of Iranian origin Shabab Ghasri had used a company in the Swedish town of Lund to export 11 very special non-corrosive valves to Iran via the United Arab Emirates. The police did not provide the details of the prosecution, but it is understood



"US Export Controls on Non-US Transactions"

plus US Export Reform Updates SEMINAR SERIES

EAR / ITAR & OFAC COMPLIANCE FOR NON-US COMPANIES

COMING TO: **SINGAPORE** MARCH 2015 **LONDON** APRIL 2015 **MONTRÉAL** MAY 2015

- Persons and Items Subject to US Jurisdiction (ITAR & EAR)
- US De Minimis Content Calculation
- US Defense Trade Controls
- Technical Data Considerations
- Enforcement Issues, Practical Advice...and MUCH MORE

Visit www.LearnExportCompliance.com/schedule
or call +1 540 433 3977 (USA) for details or registration.

that a Lund company was the exporter and the UAE was the (falsely-described) destination of end use.

Ghasri denied any criminal charges and claimed that the valves were intended for end use in the oil and gas industry. According to experts at ISP, the valves could be used in the oil and gas industry and in other sectors, but the properties of the materials are so advanced that there is no point in using them for such purposes.

But had Ghasri attempted to export unlisted valves possessing similar qualities, we see the following problems arising:

- The valves are unlisted, so there is no need to prove the end use in the form of any end-user certificate;
- This type of valve is so commonly used in different sectors of industry that there is unlikely to be a need for falsification of the destination country for end use;
- These valves are indeed used in the oil and gas industry, so their export will attract less attention than exports of specific devices.

Phase 2

According to court documents, Ghasri didn't apply for permission to export such valves and also violated international sanctions on Iran. This case was discovered when Swedish customs officials made a random check on a shipment.

If we again apply such scenario to a case of unlisted valves exports, we can see:

- These valves aren't included in control lists of dual-use items which means the exporter does not need to obtain an export licence;
- Checks of shipments of unlisted dual-use valves will be unlikely to identify this as an illegal export because there is usually nothing suspicious about such a shipment.

Phase 3

If the exported items are unlisted and do not require any licence for export, they still can fall within the scope of the catch-all mechanism described in Article 4 of EC Regulation №428/2009. In this case, in Sweden, the penalty for export without permission is the same as that for illegal export of controlled dual-use items. But the main problem here lies

Contrasting scenarios: real life vs case study		
	Real-life case of illegal export to Iran	Our possible analysed valve export
Dual-use item	Gas control valve subject to export control	Common unlisted stainless steel gas control valve
Possible WMD end use	Uranium enrichment	Uranium enrichment
Possible civil end use	Oil and gas industry	Oil and gas industry
Application for export licence	Was not applied for	No requirement
End-user commitments	Were not made	No requirement
Transporting to the client	Difficult to conduct	Can easily be conducted due to common availability of valve type
Weak point in proliferators' plan	Random check of shipment by customs	No: shipment checks do not block export
Result	Exports stopped	Exports can proceed

in proving that the exporter did indeed know about any possible WMD use of the exported items. Indeed, linking an exporter with a WMD programme is one of the greatest challenges faced by export control regimes nowadays.

This can be shown in the diagram 'Contrasting scenarios', above.

Conclusion

The valves we analysed are not initially subject to export controls. But it is critically important to prevent any exports that can lead to proliferation of dual-use technologies. The authors suggest a set of measures contributing to the solution of this problem.

- Greater focus on licensing procedures;
- Updating dual-use control lists (where possible), making them stricter and more comprehensive;
- Wider use of general licences (as described in Russian) and global licences (EU) in order to soften the negative influence on national exports caused by tightening export controls;
- Effective intelligence work;
- Greater interaction with intelligence agencies in order to prevent any proliferation scenarios, such as one described in the case study;
- Tighter control of end use of dual-use items as much as it possible;

- Strengthening the detection, suppression and prosecution of illegal activities;

Ongoing and comprehensive enforcement of dual-use export controls is critically important in the fight against proliferators. Early prevention of proliferating exports is more effective than detection at the border. Strengthening national dual-use export licensing systems is especially significant.

*Elisey Andreevsky is a former officer of the Security Service in the Leningrad nuclear power plant (Saint-Petersburg, Russia) and a 2012 intern of the Stockholm International Peace Research Institute. Yuriy Daneykin, is the acting director of the Division of Academic Methodology in the National Research Tomsk Polytechnic University (Tomsk, Russia).
eliseyandreevsky@mail.ru
daneykin@tpu.ru*

WorldECR

The journal of export controls and compliance

Contributors in this issue

Jaewon Lee, Science and Technology Policy Institute,
Sejong, Korea

writejaewon@gmail.com

Reid Whitten, Sheppard Mullin

www.sheppardmullin.com

Doron Hindin, Herzog Fox & Neeman

www.hfn.co.il

Adam Weber, Elena Hushbeck, Emily Rosenblum,
Jay Johnson, Joe Petersen and Pete Heine, Center for
Strategic Security, Argonne National Laboratory
www.gss.anl.gov/center-for-strategic-security-overview

Elisey Andreevsky and Yuriy Daneykin

eliseyandreevsky@mail.ru; daneykin@tpu.ru

WorldECR Editorial Board

Michael Burton, Jacobson Burton PLLC

mburton@jacobsonburton.com

Larry E. Christensen, Miller & Chevalier, Washington, DC

lchristensen@milchev.com

Iain Macvay, King & Spalding, London

imacvay@kslaw.com

The Honorable Mario Mancuso, Fried Frank, Harris,
Shriver & Jacobson LLP, Washington, DC

mario.mancuso@friedfrank.com

Dr. Bärbel Sachs, Noerr, Berlin

baerbel.sachs@noerr.com

Edmund Sim, Appleton Luff, Singapore

sim@appletonluff.com

George Tan, Global Trade Security Consulting, Singapore

georgetansc@sg-gtsc.com

Stacey Winters, Deloitte, London

swinters@deloitte.com

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

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

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

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

WorldECR is published by D.C. Houghton Ltd.

Information in WorldECR is not to be considered legal advice. Opinions expressed within WorldECR are not to be considered official expressions of the publisher. The publisher assumes no responsibility for errors and omissions appearing within. The publisher reserves the right to accept or reject all editorial and advertising matter. The publisher does not assume any liability for unsolicited manuscripts, photographs, or artwork.

***Single or multi-site: Do you have the correct subscription?** A single-site subscription provides WorldECR to employees of the subscribing organisation within one geographic location or office. A multi-site subscription provides WorldECR to employees of the subscribing organisation within more than one geographic location or office. Please note: both subscription options provide multiple copies of WorldECR for employees of the subscriber organisation (in one or more office as appropriate) but do not permit copying or distribution of the publication to non-employees of the subscribing organisation without the permission of the publisher. For full subscription terms and conditions, visit <http://www.worlddec.com/terms-conditions>

For further information or to change your subscription type, please contact Mark Cusick - mark.cusick@worlddec.com

© D.C. Houghton Ltd 2015. All rights reserved. Reproduction in whole or in part of any text, photograph, or illustration without express written permission of the publisher is strictly prohibited.

ISSN 2046-4797. Refer to this issue as: WorldECR [0039]

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

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482)
with its registered office at 145 - 157 St John St, EC1V 4PY, London, UK

ISSUE 39. APRIL 2015
www.WorldECR.com